WINDOWS DESKTOP APPLICATION

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 3, Release 1

09 March 2007

Developed by DISA for the DoD

This page is intentionally left blank.

SUMMARY OF CHANGES

GENERAL CHANGES:

Overall document explicitly states it applies to servers as well as workstations.
Updated Mobile Code Guidance based on updated Category Risk Assignments. See *Appendix A, Related Publications* for the reference document.
Added a List of Tables.

SECTION 1. INTRODUCTION

Updated Section 1 with information concerning scope.
Updated Severity Code definitions to be more technology specific.

SECTION 2. GENERAL INFORMATION

Updated 2.1 to add a definition of Disabled.
Updated 2.4 to include Freeware and Shareware information.

SECTION 3. GENERAL APPLICATION/WINDOWS GUIDANCE

Updated Mobile Code Guidance based on updated Category Risk Assignments.
Updated section 3.2 to include other real time communication guidance.

SECTION 4. ANTI-VIRUS SOFTWARE

Updated DTAG014 – added a requirement to have a notification mechanism for SAs or IAOs in the case of virus detection.
Updated DTAG011- added USB drives.
Updated DTAG013- to be at 30 days.

SECTION 5. WEB BROWSERS

DTBG009 – Updated the requirement from notification from any switch to or from a secure to a non-secure site to warn only before switching from a secure site to a non-secure site.
DTBG010 – Updated to include sub root level certificates.
DTBG012 – Updated to be CAT I.
DTBG016 – Updated for clarification of the allowed channel.
DTBG018- DTBG021 – New requirements.
Updated Mobile Code Guidance based on updated Category Risk Assignments.

SECTION 6. E-MAIL CLIENTS

No updates**.**

SECTION 7. OFFICE AUTOMATION SUITES

No updates.

SECTION 8. SECURING REMOTE DEVICES

Moved Securing Remote Devices to Section 9.
SRC410 – Updated with additional Mobile Code Guidance
SRC570 – Updated based on new policy guidance for protection of sensitive data
SRC605 and SRC606 - new requirements

SECTION 8. ANTISPYWARE

Added new section.

APPENDIX B. ANTIVIRUS PRODUCT SPECIFIC GUIDANCE

Updated Guidance for McAfee Version 8.x and Symantec Version 10.x.

APPENDIX C. WEB BROWSER PRODUCT SPECIFIC GUIDANCE

Updated Java Guidance for Internet Explorer
Added Section C.3 FireFox.

APPENDIX E. OFFICE AUTOMATION PRODUCT SPECIFIC GUIDANCE

Added a new requirement for CustomerExperience Program (DTOO004).

TABLE OF CONTENTS

Page

LIST OF TABLES

1. INTRODUCTION

This *Windows Desktop Application Security Technical Implementation Guide (STIG)* provides the technical security policies, requirements, and implementation details for applying security concepts to Commercial-Off-The-Shelf (COTS) applications.

The nearly universal presence of systems on the desktops of all levels of staff provides tremendous opportunities for office automation, communication, data sharing, and collaboration. Unfortunately, this presence also brings about dependence and vulnerabilities. Malicious and mischievous forces have attempted to take advantage of the vulnerabilities and dependencies to disrupt the work processes of the Government. Compounding this problem is the fact that the vendors of software applications have not expended sufficient effort to provide strong security in their applications. Where applications do offer security options, the default settings typically do not provide a strong security posture.

Given the very large set of applications, environments, and implementation strategies, it is not possible to adequately cover every instance. This document provides general guidance on some of the commonly found desktop applications in the most commonly found desktop operating system environments. Web browsers and e-mail clients were given priority, because they are most common. Anti-virus products, because of their strategic importance in preventing problems, were also a priority. Other applications were added as specific requirements were identified. Appendices exist that apply the general guidance to specific products and versions of commonly found applications. For applications not specifically defined in the Appendices, guidance from the general section should be used to secure the application.

1.1 Background

Even though this document addresses the security of COTS applications rather than an operating system, it is not possible to completely separate the security issues. Security is an attribute of the whole as well as of each of the parts. In accordance with this philosophy, the same policies and guidance that apply clearly to operating systems are also applicable to applications.

The applications addressed in this document utilize mobile code and Public Key Infrastructure (PKI) technologies to enable some of their features. The requirements described in this document are designed to implement the applicable DoD polices for those technologies. These policies are described in the *Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems*, (later referred to as the DoD Mobile Code Policy) and the *Department of Defense Instruction, "Department of Defense (DoD) Public Key Infrastructure (PKI) and Public Key (PK) Enabling* documents referenced in *Appendix A, Related Publications*.

1.2 Authority

DoD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines" and tasks Defense Information Systems Agency (DISA) to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DoD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DoD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing sensitive information.

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The IAO will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

It should be noted that Field Security Operations (FSO) support for the STIGs, Checklists, and Tools is only available to DoD Customers.

1.3 Scope

The requirements and recommendations set forth in this document will assist Information Assurance Officers (IAO) and Information Assurance Managers (IAM) in protecting desktop applications in DoD locations hereafter referred to as sites. The responsible Configuration Control Board (CCB) will approve revisions to site systems that could have a security impact. Therefore, before implementing Desktop Application security measures, the IAO or TASO will submit a change notice to the CCB for review and approval.

Although there are a few different operating system platforms for desktop environments, this document addresses applications running on Windows platforms. This document does not include specific guidance for Unix or Linux desktop environments at this time.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**". The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" indicates mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written.

For each italicized policy bullet, the text will be preceded by parentheses containing the STIG Identifier (STIGID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows: "(*G111: CAT II*)." If the item presently does not have an STIGID, or the STIGID is being developed, it will contain a preliminary severity code and "N/A" (i.e., "*[N/A: CAT III]*"). Throughout the document accountability is directed to the IAO to "ensure" a task is carried out or monitored. These tasks may be carried out by the IAO or delegated to someone else as a responsibility or duty.

A reference to "**should**" indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. All reasonable attempts to meet this criterion will be made.

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall. This includes a vulnerability that would allow execution of Category 1X mobile code and unsigned Category 1A mobile code
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder. This includes inappropriate execution of Category II mobile code.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.

Table 1-1. Vulnerability Severity Code Definitions

1.6 DISA Information Assurance Vulnerability Management (IAVM)

The DoD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DoD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) web site: https://www.jtfgno.mil.

1.7 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.8 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

2. GENERAL INFORMATION

This STIG has set forth requirements based upon having a secured Windows environment as described in various other documents. These documents include various NSA Guides (http://www.nsa.gov/snac/) and the Windows/2000/XP/2003 Addendum available from the Information Assurance Support Environment (IASE) (http://iase.disa.mil/) web site. The superset of these requirements can be found in the appropriate Windows Checklist also available from the IASE. Failure to follow these requirements can significantly diminish the value of many of the specifications in this document.

Security controls that are managed through the underlying operating system platform directly affect the strength of the security that surrounds desktop applications. This section highlights some measures that are taken to increase that strength.

This section of the document provides the following categories of information:

- Considerations for the terminology and content of this document

- Information relevant to general desktop application security that is not specific to an individual product

- Limited guidance on individual products or categories of products that are not covered in subsequent chapters

2.1 Terminology Conventions

Current desktop applications present a graphical user interface (GUI) for their use and parameter customization. Most of the parameter settings specified in this document can be examined and changed through the application's GUI, subject to Windows policy settings. The following terms are used in describing how to view or configure the settings:

- Dialog – An application dialog is a window presented by the application.

- Menu – An application menu consists of a textual list of actions, commands, or (sometimes) options that can be selected.

- Enable – The term enable is used to describe the selection of a parameter setting, often indicated as an option button or check box in the application GUI. For example, when a parameter setting specifies, "enable", the associated option button display would indicate that the option is selected.

- Disable – The term disable is used to describe the de-selection of a parameter setting, often indicated as an option button or check box in the application GUI. For example, when a parameter setting specifies, "disable", the associated option button display would indicate that the option is de-selected.

2.2 Compliance Checking

In the individual application chapters of this document, instructions are provided to explain a manual method of viewing or changing parameter settings. These instructions generally involve the use of application dialogs that present the information graphically. It should be noted that these manual instructions are not intended for use in a general compliance checking process. The compliance checking process utilizes automated procedures that are documented in the associated checklist.

2.3 Other Considerations

It must be noted that the guidelines specified should be evaluated in a local, representative test environment before implementation within large user populations. The extensive variety of environments makes it impossible to test these guidelines for all potential software configurations. For some environments, failure to test before implementation may lead to a loss of required functionality.

2.4 Open Source / Freeware

DoD has clarified policy on the use of open source software to take advantage of the capabilities available in the Open Source community as long as certain prerequisites are met. DoD no longer requires that operating system software be obtained through a valid vendor channel and have a formal support path, if the source code for the operating system is publicly available for review.

DoD CIO Memo, "Open Source Software (OSS) in Department of Defense (DoD), 28 May 2003":

> "DOD Components acquiring, using or developing OSS must ensure that the OSS complies with the same DOD policies that govern Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) software. This includes, but is not limited to, the requirements that all information assurance (IA) or IA-enabled IT hardware, firmware and software components or products incorporated into DOD information systems whether acquired of originated within DOD:
>
> Comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 and be configured in accordance with DOD-approved security and configuration guidelines at http://iase.disa.mil/ and http://www.nas.gov/."

Open source software takes several forms:

1. A utility that has publicly available source code is acceptable.

2. A commercial product that incorporates open source software is acceptable because the commercial vendor provides a warranty.

3. Vendor supported open source software is acceptable.

4. A utility that comes compiled and has no warranty is not acceptable.

The DoDD 8500.1 says “Public domain software products, and other software products with limited or no warranty, such as those commonly known as freeware or shareware, shall only be used in DoD information systems to meet compelling operational requirements. Such products shall be thoroughly assessed for risk and accepted for use by the responsible DAA.”

3. GENERAL APPLICATION/WINDOWS GUIDANCE

This section of the document provides general guidance for products or categories of products that are not covered in subsequent chapters.

3.1 Data Backup

Data integrity and availability are key security objectives. Adequate data backup is one strategy that is crucial to meeting these objectives. Although users of desktop applications may not be creating mission critical data, all their data represents a resource that, if lost, could result in a permanent loss of information or productivity.

A backup strategy is highly dependent on the physical and logical environments. In environments where users frequently operate disconnected from a LAN, as in the case of notebook PC users who travel, it is not generally practical for the users to store all their data on a file server. Developers may require standalone copies of program code while additions or alterations are in progress. For these and other reasons, strict requirements for desktop backup are not addressed in this document. However, this section does provide recommendations that should be considered.

Users should make conscious decisions about the physical location where desktop application data is stored. They should be aware of the backup policy for that location. Any backup policy should be implemented in accordance with the following:

- Mission critical data should be stored on file servers with a formal data backup policy. Storage of mission critical data on desktop machines should be considered temporary.

- To the greatest extent possible, data files should be stored in a directory hierarchy that is separate from program files.

- An incremental, or change-based, backup solution can be used daily.

- A full data backup solution should be used at least weekly.

- Use of a Compact Disk-Recordable (CD-R) or Compact Disk-ReWritable (CD-RW) drive should be considered for desktop machines. CD-R and CD-RW disks provide high capacity at relatively low cost.

- The backup data should be stored on media or another machine that is not physically close to the original data source.

- Backup media should receive proper care according to its characteristics. Regular rotation of tape media is necessary to ensure usability. The media should be clearly labeled, including any appropriate security classification marking.

- Backup tools and schedules should be documented.

- Restoration tools and methods should be documented and they should be tested via restoration at least annually.

- *(DTGW001: CAT II) The SA will ensure an appropriate data backup strategy exists and is executed based upon the machine use and nature of the data.*

3.2 Instant Messaging (IM) Clients and Voice or Video over IP services

Instant Messaging or IM clients provide a way for a user to send a message to one or more other users in real time. Additional capabilities may include file transfer and support for distributed game playing. Communication between clients and associated directory services are managed through messaging servers. Commercial IM clients include AOL Instant Messenger (AIM), MSN Messenger, and Yahoo! Messenger, and Skype. The Windows XP operating system includes the Windows Messenger component as an IM client. (This should not be confused with Windows Messaging which is a service within Windows.)

IM clients present a security issue when the clients route messages through public servers. The obvious implication is that potentially sensitive information could be intercepted or altered in the course of transmission. This same issue is associated with the use of public e-mail servers.

In order to reduce the potential for disclosure of sensitive Government information and to ensure the validity of official government information, IM clients that connect to public instant messaging services will not be installed.

- *(DTGW002: CAT II) The SA will ensure public instant messaging clients are not installed.*

NOTE: Clients used to access an internal or DoD controlled IM applications are permitted.

- *(DTGW006: CAT II) The SA will ensure instant messaging clients that are used for an internal or DoD controlled IM application are at the current patch level.*

Yesterday's separate voice and data communications infrastructures are morphing into a single infrastructure based upon the data network and its transition into the Internet and World Wide Web. This infrastructure is based upon the IP protocol and the name of this transition process is called "convergence". The vision is that one day all forms of communications will ride a single "Net Centric", "Converged" network. Voice and Video communications are also referred to as being Real Time Services (RTS)

Part of this convergence is the development and use of desktop applications that can turn a workstation (desktop or laptop) into a phone or a Video Teleconferencing (VTC) terminal. This is accomplished by the simple addition of a headset, microphone, and in the case of VTC, a camera. The camera is otherwise known as a "Web Cam". These applications are referred to as "Soft Phones" or "Soft VTC terminals" since they are software based. Similar applications and peripheral attachments have recently become popular in Instant messaging (IM) applications. Some "Collaboration Tool Suites" are based upon IM and also provide full VTC capabilities along with the classic document (data based) collaboration.

Special consideration must be given to workstation and desktop application security as well as the network architecture that support RTS systems for, both the protection of the "data" on the network and the RTS using it. Workstation based Voice and VTC applications works against the security measures and protections used in the network infrastructure to protect these modes of communication.

Please refer to the *DoD Voice and Video Communications / Real Time Services (RTS) STIG* for the additional security requirements and guidance related to the implementation of Soft Phones and Soft VTC applications on workstations.

- *(DTGW007: CAT II) The SA will ensure VOIP or VTC clients that access public services are not installed.*

3.3 Peer-to-Peer File-Sharing Utilities and Clients

File-sharing utilities and clients can provide the ability to share files with other users (Peer-to-Peer Sharing). This type of utility is a security risk due to the potential risk of loss of sensitive data and the broadcast of the existence of a computer to others. There are also many legal issues associated with these types of utilities including copyright infringement and intellectual property issues. These types of utilities and clients include the following examples, Napster, Gnutella, Kazaa, and Freenet.

- *(DTGW003: CAT II) The SA will ensure peer-to-peer file-sharing clients are not installed.*

NOTE: Clients used to access an internal or DoD controlled file-sharing system are permitted.

3.4 Microsoft SQL Server Desktop Engine (MSDE)

The Microsoft SQL Server Desktop Engine (MSDE) is a database manipulation tool intended for Windows desktop computers. It is packaged with Microsoft applications such as Office, Visio, and Application Center. An earlier version of MSDE was known as the Microsoft Data Engine. MSDE shares a common technology base with the Microsoft SQL Server product that runs on Windows servers.

Please refer to the *Database Security Technical Implementation Guide* for actions that are required to secure MSDE.

3.5 Windows File Type Handling Properties

The Windows operating system supports the definition of file types based on file name extensions. These definitions, located in the Windows Registry, can include a number of properties that specify how files are manipulated.

Because many file types may contain some form of program code, vulnerabilities can be introduced when the files are delivered over a network through web browser or e-mail clients.

E-mail clients use the Windows File Type Associations to invoke an application to open e-mail attachments. In addition, in some circumstances (e.g., URL that is a file reference, within HTML web page) browsers use the Windows File Type Associations to invoke the specified application to open the downloaded file contents and execute any embedded mobile code. The DoD Mobile Code Policy prohibits the execution of some mobile code (Category 1X) in some applications in this manner (e.g., Windows Scripting Host [wscript.exe, cscript.exe], and Microsoft HTML Application Host [mshta.exe]).

The Windows file type-handling properties Actions, Open Confirmation, and Always Show Extension can be used to help control Windows behavior for files that may contain executable code.

- The Actions property defines tasks and the applications that perform these tasks for the related file type. Open and Edit are the most common tasks. Typically Actions are defined when the applications that perform those actions are installed. One of the defined Actions can be designated as the default action for the file type. Windows Explorer, Internet Explorer, and Outlook are common applications that invoke the default file type Action when a file (by name or icon) is opened (e.g., double clicked) in the application. Some applications from other vendors use these definitions as well.

- The Always Show Extension property specifies whether the file extension is displayed when the file name is displayed. Displaying the file extension provides a visual cue that a file may contain mobile code. This facility can help educated users to avoid opening potentially dangerous e-mail attachments. For example, the Anna K virus attempted to deceive users into thinking that they were opening a safe image file rather than a malicious VBScript file by naming the e-mail attachment ‘photo.jpg.vbs’, when the file extension is not displayed, the filename appears to be photo.jpg.

- The Open Confirmation property specifies whether a warning is issued before a downloaded file is opened. This facility gives users a warning and a chance to cancel the file open operation.

The DoD Mobile Code Policy prohibits the execution of the following types of Category 1X mobile code:

a. All mobile code that executes in Windows Scripting Host (i.e., scripts executing in wscript.exe or cscript.exe).
b. Scrap objects
c. HTML Applications (i.e., hta files executing in mshta.exe)
d. MS-DOS batch files and UNIX Shell scripts

The DoD Mobile Code Policy also requires that the automatic execution of all types of mobile code in e-mail bodies and attachments be disabled; and that the user must be prompted prior to opening e-mail attachments that may contain mobile code. The Windows File Type Associations settings are configured to implement some of these requirements as described below.

3.5.1 File Type Handling Properties – Preventing Code Execution

For certain file types, it is necessary to take steps to ensure that the default method of opening the file does not allow mobile code to be executed. Two techniques to achieve this goal are discussed here—altering the default file type Action and deleting the file type definition. Although methods of removing Microsoft's Windows Script Host (WSH) component might meet most of this requirement, that technique should not be the first choice. It would disable functionality that might be in use for other purposes, and the specific method used would have to be compatible with the Windows File Protection (WFP) feature present in later versions of Windows.

The default Action property can be altered to change the standard default Action from Open to Edit. When this technique is used, instead of executing a program with the file contents as code, an editor is opened with the file contents as a document. For example for a .vbs file, the Open action may be the command 'C:\WINNT\System32\Wscript.exe "%1" %*' and the Edit action may be the command 'C:\WINNT\System32\Notepad.exe "%1" %*'. Changing the default action to Edit results in a Notepad window opening up instead of the file being executed by the Windows Scripting Host when the .vbs file is opened. For non-technical user communities, an alternative that may be more appropriate is to have the Edit action be the command 'C:\WINNT\System32\Notepad.exe "C:\MC_Warn.txt"', where the file C:\MC_Warn.txt is created locally and contains a warning that the user has attempted to open a potentially dangerous file.

When altering the default file type Action is the technique used, the Always show extension setting adds additional value. This ensures that users can see the file type before attempting to open it.

While the alternate technique of deleting existing Windows file type definitions does provide security, it is not always a more secure long-term solution. During maintenance or product installation, a non-existent file type is usually defined while existing file type properties are usually not overwritten.

Regardless of which technique is used, the significant result is that when an attempt is made to open certain files using default application actions, any code in the file is not executed.

- *(DTGW004: CAT II) The SA will ensure if any of the file types in the following table are defined to Windows, the settings for each file type are configured as follows:*

  - *The default Actions for 'Edit' and 'Open' are changed to an application that does not execute the code in the file.*

  - *The 'Always show extension' setting is enabled.*

WINDOWS FILE DEFAULT ACTION AND SHOW EXTENSION UPDATES	
FILE TYPE	***EXTENSION***
JScript Encoded File	*JSE*
JScript File	*JS*
HTML Applications as Mobile Code	*HTA*
Shell Scrap Object	*SHS, SHB*
VBScript Encoded File	*VBE*
VBScript File	*VBS*
Windows Script Component	*WSC, SCT*
Windows Script File	*WSF*
Windows Script Host Settings File	*WSH*

Table 3-1. Windows File Default Action and Show Extension Updates

As mentioned earlier, it is possible to meet this requirement by deleting the file type definitions. When using either technique, the SA must ensure that the installation of program maintenance or new programs does not cause unsafe file definitions to be re-created.

Many of these file types are associated with Microsoft's Windows Script Host (WSH) component. It is possible that additional file types might also be associated with it. Updates to any additional file types are recommended. The additional file types can be determined by scanning the HKEY_CLASSES_ROOT section in the Windows Registry for references to wscript.exe and cscript.exe.

3.5.2 File Type Handling Properties – Confirming Code Execution

For some file types, providing the user an opportunity to cancel the opening of the file provides adequate protection for most environments. Files that are opened with applications that include internal controls on code execution are good candidates for this technique.

The Open Confirmation property, enabled through the Confirm open after download setting, provides a notice to the user that allows them to open the file, save the file to disk, or cancel the file open task. The Always show extension setting adds additional value. This ensures that users can see the file type before attempting to open it.

- *(DTGW005: CAT II) The SA will ensure if any of the file types in the following table are defined to Windows, the settings for each file type are configured as follows:*

  - *The 'Confirm open after download' setting is enabled.*

  - *The 'Always show extension' setting is enabled.*

WINDOWS FILE OPEN CONFIRMATION AND SHOW EXTENSION UPDATES	
FILE TYPE	***EXTENSIONS***
JScript Encoded File	*JSE*
JScript File	*JS*
HTML Applications as Mobile Code	*HTA*
Shell Scrap Object	*SHS, SHB*
VBScript Encoded File	*VBE*
VBScript File	*VBS*
Windows Script Component	*WSC, SCT*
Windows Script File	*WSF*
Windows Script Host Settings File	*WSH*
Adobe Acrobat Document, Forms Document	*PDF, FDF, XFDF*
LotusScript Library, Object, Source	*LSL, LSO, LSS*
Microsoft Excel Web Query File, OLE DB Query File, Backup File, Worksheet, Template	*IQY, RQY, XLK, XLS, XLT*
Microsoft PowerPoint Template, Slide Show, Presentation	*POT, PPS, PPT*
Microsoft Word Document, Template, Backup Document	*DOC, DOT, WBK*
MS-DOS Batch File	*BAT*
PostScript	*PS, EPS*
Rich Text Format	*RTF*
WordPerfect (PerfectScript) Coach, Macro	*WCH, WCM*
VISIO	*VSS, VST, VSD, VSW*
Microsoft Access	*AD, ADP, MDB, MDE*
Shockwave	*DCR, DXR, DIR, SPL, SWF*
Flash	*FLS,*

Table 3-2. Windows File Open Confirmation And Show Extension Updates

Updates should also be performed to any additional Microsoft Access, Excel, PowerPoint, and Word file types and to any other file types for files that could potentially contain mobile code.

3.5.3 File Type Handling Properties – Manual Display and Configuration

The command line tool, 'assoc', can be used to determine if a given file type definition exists. For example, on typical Windows systems the command 'assoc.bat' returns '.bat=batfile' indicating that the extension .bat is defined and that the properties are stored in the Windows Registry under the key batfile.

Windows Explorer can be used to manually display and configure the Actions, Always Show Extension, and Open Confirmation properties. In Windows 2000 and XP use the File Types tab of the Tools | Folder Options dialog in Windows Explorer.

It must be recognized that performing these changes does not eliminate the danger from malicious code. Such code could come from a number of sources and use trigger techniques other than the Windows file type open action. Thus the changes documented here are not a substitute for an anti-virus tool with current definitions.

NOTE: The application of this change affects the behavior of all Windows applications that utilize the affected Registry settings.

4. ANTI-VIRUS SOFTWARE

Next to properly configured operating system security controls, effective anti-virus software is the most critical tool in securing desktop systems. The value of up-to-date software with current virus definition files cannot be underestimated. Malicious programs that result in a denial of service or corruption of data can be thwarted with anti-virus programs that look for signatures of known viruses and take preventative action.

- *(DTAG001: CAT I) The SA will ensure every machine has an anti-virus program installed and active for on-access and on-demand virus detection.*

NOTE: The use of products by DoD organizations, other than those available on the JTF-GNO web site, is discouraged. DoD has special licensing agreements with both McAfee and Symantec.

It must be noted that the guidelines in this section have been written to apply to clients whether on a server or workstation. Using these guidelines for mail servers does not provide appropriate or adequate protection for servers running complex applications such as MS Exchange or Lotus Notes. Additional antivirus measures need to be taken on mail servers.

The JTF-GNO makes several anti-virus tools available for download from their web site at https://www.jtfgno.mil/antivirus/av_info.htm. These products are also available for download on the DoD Patch Repository at https://patches.csd.disa.mil. Specific product guidance for the JTF-GNO NetDefense provided client products can be found in Appendix B.

The following sections provide general guidance that applies to all anti-virus software. It defines the principles that are applied in the software-specific requirements that are described in Appendix B. If there is a requirement to use software that is not covered in the Appendix, the guidance in this section applies.

4.1 Software Maintenance

- *(DTAG002: CAT I) The SA will ensure the anti-virus software installation is a supported version.*

- *(DTAG003: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading anti-virus software prior to the date the vendor drops security patch support.*

- *(DTAG004: CAT II) The SA will ensure the latest maintenance rollup or software update for the anti-virus software is applied.*

- *(DTAG005: CAT II) The SA will ensure anti-virus software installation and update files are only downloaded from a trusted site such as the JTF-GNO NetDefense or directly from the vendor's site.*

- *(DTAG006: CAT II) The SA will ensure anti-virus definition/signature files are automatically updated at least weekly.*

NOTE: It is recommended the signatures be updated daily.

- *(DTAG007: CAT II) The SA will ensure standard procedures exist and are executed for updating anti-virus definition/signature files on isolated networks or standalone systems at least weekly.*

- *(DTAG008: CAT I) The SA will ensure signature files are no older than 14 days.*

NOTE: In the event that JTF-GNO NetDefense does not release a signature file in the last 14-day period, then the most current release is required.

- *(DTAG009: CAT II) The SA will ensure Beta or non-production versions of definition/signature files are not used on production machines.*

4.2 General Guidance for Anti-virus Software

This section details general guidance for the configurations of anti-virus products.

- *(DTAG010: CAT II) The SA will ensure anti-virus software is configured to start on-access protection automatically when the Windows Operating system is booted.*

- *(DTAG011: CAT II) The SA will ensure anti-virus software is configured to perform a virus scan of the local hard drives at least weekly.*

NOTE: Scans at boot time (or daily) are recommended when this would not cause a significant impact to operations.

The following file types are particularly vulnerable as the host for a virus. These file types must be included in the anti-virus scan:

- Executable, service, and driver files (i.e., files suffixed with .bat, .bin, .com, .dll, .exe, .sys, etc.)

- Application data files that could contain a form of mobile code (i.e., files suffixed with .doc, .dot, .rtf, .xls, .xlt, hta, scrap objects, wsh ,etc.)

- *(DTAG012: CAT II) The SA will ensure, at a minimum, anti-virus software is configured to scan the required file types in all directories except those used to hold files quarantined by the anti-virus software.*

- *(DTAG013: CAT II) The SA will ensure anti-virus software is configured to scan files incoming from floppy disks, e-mail attachments, web site downloads, and any other locally attached devices such as Zip Drives, USB Drives or Personal Digital Assistants.*

NOTE: This requirement also includes activation of any e-mail client or web browser interface provided by the anti-virus software.

In the event that a virus is found, the user must be notified. This allows the user to take any additional action to reduce damage and halt propagation of the virus. The user should also exercise the appropriate computer security incident reporting requirements as defined by the site.

- *(DTAG014: CAT II) The SA will ensure the anti-virus software, when running in on-access mode, is configured to inform the user and have a mechanism to notify the SA or IAO at the time a virus is detected.*

- *(DTAG015: CAT II1) The SA will ensure the anti-virus software is configured to maintain anti-virus log files for at least 30 days.*

This page is intentionally left blank.

5. WEB BROWSERS

Web browsers are the client applications that communicate with web servers. Because early versions were available at low or no cost and because they are now bundled with operating systems of all types, browsers are now installed on practically every computer. The proliferation of web sites and the associated easy access to information have made web browsers critical business applications.

It must be noted that the requirements in this section have been written to apply when machines are acting as clients. On server platforms, the security configuration parameters will be set to at least as restrictive values as those listed in this section. When practical, web browsers should not be installed on servers. However, due to the implementation of shared components and use in administering other server software components, it is usually not practical to remove all browsers on server platforms.

As with other widely available, highly used software products, web browsers have become common targets for people intending to disrupt business processes. The following types of attacks are commonly used:

- Data, HTML web pages, and files sent to the browser can contain mobile code that can damage both user and system files on the client computer. Damage can range from simple disruption to alteration and permanent data loss.

- Data, HTML web pages, and files sent to the browser can contain mobile code that can cause the disclosure of data stored on the client or a weakening of client security so that other attempts to acquire data can be successful. Malicious mobile code can collect data, passwords, and other sensitive information (e.g., user's keystrokes) and send it to a remote host.

- Data, HTML web pages, and files sent to the browser can contain mobile code that spawns some form of attack on other clients or servers by propagating malicious code or by creating conditions that can result in a denial-of-service (DoS).

Web browsers enable technologies that support the execution of mobile code and utilize PKI technologies to support some features. The requirements described in this document are designed to implement the applicable DoD polices for those technologies. These policies are described in the *Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems*, (later referred to as the DoD Mobile Code Policy) and the *Department of Defense Instruction, Department of Defense (DoD) Public Key Infrastructure (PKI) and Public Key (PK) Enabling* documents referenced in *Appendix A, Related Publications*.

The following sections provide general guidance that applies to all web browsers. Product specific guidance can be found in Appendix C. If a product is being used that is not included, these general guidelines should be used to configure the browser.

5.1 Software Maintenance

Maintaining the security of web browsers requires frequent reviews of security bulletins. Many security bulletins mandate the installation of a software patch to overcome security vulnerabilities.

SAs and IAOs should regularly check browser vendor web sites for information on new security patches that are applicable to their site. All applicable security patches will be applied to the system. Security patches are deemed applicable if the product is installed, even if it is not used or is disabled.

FSO does not test or approve patches or service packs. It is the site's responsibility to test vendor patches within their test environment.

- *(DTBG001: CAT II) The IAO will ensure all browser security related software patches are applied and documented.*

- *(DTBG002: CAT II) The IAO will ensure the latest maintenance rollup or service packs for the browser are applied and documented.*

NOTE: Generally a couple of months will be allowed for any problems to be reported to the vendor prior to new maintenance rollup or service packs being required.

SAs and IAOs should regularly check browser vendor web sites for information concerning products or versions of products no longer being supported. Action should be taken to ensure a smooth migration plan is developed and implemented prior to a product going into a nonsupport status.

- *(DTBG003: CAT I) The IAO will ensure unsupported browser software is removed or upgraded prior to a vendor dropping support.*

- *(DTBG004: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading browser software prior to the date the vendor drops security patch support.*

Many software vendors are offering services that provide for automatic installation of patches. This service should be disabled to prevent users from downloading and installing updates that have not been approved and tested by the site. Many vendors have also implemented features that will send an error report to the vendor. This type of feature will be disabled.

- *(DTBG006: CAT II) The SA will ensure options that automatically report errors back to the vendor are disabled.*

5.2 Secure Browser Sessions and Digital Certificates

The capability for secure sessions between web browsers and servers is essential. A common method of securing sessions is the use of a protocol that provides data integrity and encryption

services. Secure Sockets Layer (SSL) is the most commonly used protocol of this type; most commercial browsers support Versions 2 and 3 of SSL. Transport Layer Security (TLS) is the successor to SSL.

To enable web browser sessions that use SSL or TLS, digital certificates are required. From an ownership perspective, there are Certification Authority (CA) certificates, server certificates, and user certificates. Although the SSL protocol specifies that user certificates are optional, security is significantly enhanced by the use of both server and user certificates. The management of digital certificates requires the use of a PKI. A discussion of PKI implementation is beyond the scope of this document. Information can be found in the *Department of Defense Instruction, "Department of Defense (DoD) Public Key Infrastructure (PKI) and Public Key (PK) Enabling* documents referenced in *Appendix A, Related Publications*.

Direction on the implementation of certificates on web servers is provided in the *Web Server Security Technical Implementation Guide*.

- *(DTBG007: CAT II) The SA will ensure browsers used to connect to Government servers are capable of 128-bit encryption and the use of SSL.*

- *(DTBG008: CAT II) The SA will ensure options applicable to the SSL protocol are configured such that it is not possible for a non-encrypted SSL session to be established.*

- *(DTBG009: CAT II) The SA will ensure options that provide warnings when a user switches from a secure (SSL-enabled) to a non-secure pages are enabled.*

The presence of specific certificates is especially important with regard to CA certificates. Because these certificates are involved in trust relationships that are used to confirm identity, it is important to verify that appropriate CA certificates for the DoD PKI are present. As of the publication date of this document, the DoD PKI is issuing Class 3 certificates. To ensure support for this environment, a check for the certificate of the DoD Class 3 Root Certificate Authority will be performed. Certificates for the DoD PKI External Certificate Authorities (ECAs) and Interim ECAs (IECAs) may be installed at the site's option.

- *(DTBG010: CAT II) The SA will ensure the certificate for the DoD Class 3 Root Certificate Authority and appropriate sublevel DoD CA Certs are installed.*

- *(DTBG011: CAT II) The SA will ensure options that provide password protection for user PKI certificates are enabled.*

5.3 Mobile Code

Mobile code is defined as "software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient." This definition and the policy for mobile code is described in the *Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems* document listed in *Appendix A, Related Publications*.

Because the web browser is a primary host for the execution of mobile code, it is critical to configure the parameters that impact mobile code execution. The following table summarizes the types of mobile code and the applicable policy:

Mobile Code Risk Category Assignments		
CATEGORY	***TECHNOLOGY***	***POLICY***
1X	Mobile code scripts executing in Windows Scripting Host (WSH) Scrap Objects* UNIX Shell scripts* MS-DOS Batch scripts* HTML Applications (i.e., .hta files) that download as mobile code Binary executables (eg. .exe files) that download as mobile code * when used as mobile code	Use of Category 1X Mobile Code is prohibited. Use of Category 1 mobile code technologies and/or products that cannot differentiate between signed and unsigned mobile code or cannot be configured to disable unsigned mobile code is prohibited; such products and/or technologies will be uninstalled or disabled from executing mobile code.
1A	ActiveX controls Shockwave movies (including Xtras)	Use of unsigned Category 1A mobile code is prohibited; download and execution of unsigned Category 1A will be disabled or technology uninstalled. Category 1 mobile code that is signed with an approved PKI code-signing certificate and obtained from a trusted source may be downloaded and executed. Web browsers and other mobile code enabled products will be configured to prompt the user prior to the execution of signed Category 1A mobile code.

Mobile Code Risk Category Assignments		
CATEGORY	***TECHNOLOGY***	***POLICY***
2	Java Applets and other Java mobile code Visual Basic for Applications (VBA) LotusScript PerfectScript Postscript Mobile code executing in the .NET Common Language Runtime	Unsigned Category 2 mobile code that executes in a constrained execution environment without access to local system and network resources (e.g., file system, Windows registry, network connections other than to its originating host) may be used. Category 2 mobile code that does not execute in a constrained execution environment may be used if obtained from a trusted source over an assured channel using one of the following: Code Signing: The mobile code was digitally signed with an approved code-signing certificate. The code-signing certificate is trusted by the recipient's component and the certificate shall be properly validated by the client prior to the mobile code being executed. SSL Connection: The mobile code was downloaded over an SSL connection from a trusted SSL web server using a DoD or trusted commercial SSL server certificate. TLS Connection: The mobile code was downloaded over a TLS connection from a trusted TLS Web server using a DoD or trusted commercial TLS server certificate. SIPRNET: The mobile code was obtained from a SIPRNET source and downloaded into a SIPRNET client via the SIPRNET. Internet Protocol Security (IPSec) Combined With Mutual Authentication: The mobile code was downloaded from a trusted web server over an encrypted IPSec

Mobile Code Risk Category Assignments		
CATEGORY	***TECHNOLOGY***	***POLICY***
		connection that establishes mutual authentication using a DoD or trusted commercial PKI certificate. To the extent possible, Web browsers and other mobile code-enabled products will be configured to prompt the user prior to the execution of Category 2 mobile code.
3	JavaScript VBScript Portable Document Format (PDF) Flash animations	May be used

Table 5-1. Mobile Code Risk Category Assignments

NOTE: The use of (a) JavaScript and VBScript scripts executing in WSH, (b) UNIX shell scripts, (c) MS-DOS batch scripts, (d) scrap objects, and (e) HTML Applications as mobile code is prohibited because these technologies cannot disable the execution of unsigned mobile code while allowing signed mobile code. However, JavaScript and VBScript scripts executing within the browser are considered Category 3 mobile code and are permitted.

Each browser has various parameters and combinations of parameters that can enforce the DoD Mobile Code Policy.

- *(DTBG012: CAT I) The SA will ensure the browser is configured to disallow execution of Category 1X mobile code.*

- *(DTBG013: CAT I) The SA will ensure the browser is configured to disallow execution of unsigned Category 1A mobile code.*

- *(DTBG014: CAT II) The SA will ensure the browser is configured to only allow signed Category IA Mobile Code that is signed from a trusted source.*

- *(DTBG015: CAT II) The SA will ensure the browser is configured to prompt for execution of signed Category 1A mobile code.*

- *(DTBG016: CAT I) The SA will ensure prohibited CAT 1X mobile code is uninstalled or disabled.*

- *(DTBG017: CAT II) The SA will ensure the browser is configured to only allow Category 2 mobile code that is signed or received from a trusted sourced over an assured channel.*

NOTE: If the Category 2 mobile code is not received over an assured secure channel from a trusted source, it must be executed within a constrained environment.

- *(DTBG024: CAT II) The SA will ensure the browser is configured to disallow mobile that has not been evaluated (emerging mobile code.).*

The browser home page parameter specifies the web page that is to be displayed when the browser is started explicitly and when product-specific buttons or key sequences for the home page are accessed. Because a web page can contain mobile code that is executed as the page is displayed, a more secure default environment is achieved when the browser's home page is set to blank**,** is one that is served from a trusted site, or is a file on a local disk drive. A trusted site may be a local site that is within the security enclave of the user or another trusted site such as the JTF-GNO NetDefense (https://www.jtfgno.mil).

- *(DTBG018: CAT II) The SA will ensure the browser's home page is set to blank, a local file, or a trusted site.*

5.4 Miscellaneous Settings

This section describes settings that cover a varying range of browser issues.

Cookies are a means that a web site can use to save state of a web application or to store information that will be resubmitted to the requesting site later in the browsing experience or during a later visit to the site. Cookie parameters need to be configured to allow current session cookies and allow cookies for originating sites only

- *(DTBG019: CAT II) The SA will ensure the browser is configured to only allow session cookies and cookies for originating sites only.*

- *(DTBG020: CAT II) The SA will ensure the browser is configured to block pop ups.*

Web sites can also change the status bar and menus. It is recommended that SAs configure the browser to constrain JavaScript and VBScript by preventing scripts from changing status bar text and from disabling or replacing context menus.

- *(DTBG021: CAT II) The SA will ensure the browser is configured to prevent scripts from changing status bar text.*

- *(DTBG022: CAT II) The SA will ensure the browser is configured to prevent scripts from changing status context menus.*

This page is intentionally left blank.

6. E-MAIL CLIENTS

E-mail is one of the primary methods for communicating information and delivering data over local and wide-area networks. As such, it is a critical business application in the contemporary workplace. The flexibility and convenience of e-mail have resulted in the presence of an e-mail client on virtually every desktop computer.

As a result of the importance of e-mail and the large installed base, those looking to disrupt business processes have targeted e-mail clients. Attacks are engineered in multiple ways:

- Message data can be designed to cause the client software to malfunction.

- Message data can contain mobile code intended to delete system or user files, modify files, forward data and sensitive user information to remote servers.

- Message data can contain mobile code intended to spawn some form of attack on other clients or servers by propagating destructive code or by creating conditions that can result in a denial-of-service.

To date, the most common method of attack is through attachments to e-mail messages. These attachments can consist of self-contained programs or script commands. The damage does not occur until the attachment is opened, triggering the execution of the malicious code.

A more recent attack technique involves the use of e-mail messages in HTML format. Malicious code is delivered through the inclusion of embedded scripts or programmatic objects (such as ActiveX controls) invoked from an HTML message. HTML in e-mail bodies or attachments can execute automatically when e-mail is previewed, causing mobile code to be automatically downloaded and executed (e.g., ActiveX control, VBScript). The damage may be done when the HTML is parsed or when it is rendered into display form. This can occur through the preview facility offered in some clients as well as when the message is opened.

The DoD Mobile Code Policy requires that the automatic execution of all mobile code in e-mail bodies and attachments will be disabled. In addition, it requires that e-mail products will be configured to prompt the user prior to opening e-mail attachments that may contain mobile code.

The following sections provide general guidance that applies to all e-mail clients. It defines the principles that are applied in the software-specific requirements that are described in Appendix D. If there is a requirement to use e-mail clients that are not covered in Appendix D, the guidance in this section applies.

6.1 Software Maintenance

Maintaining the security of e-mail requires frequent reviews of security bulletins. Many security bulletins mandate the installation of a software patch to overcome security vulnerabilities.

SAs and IAOs should regularly check vendor web sites for information on new security patches that are applicable to their site. All applicable security patches will be applied to the system. A security patch is deemed applicable if the product is installed, even if it is not used or is disabled.

FSO does not test or approve patches or service packs. It is the site's responsibility to test vendor patches within their test environment.

- *(DTMG001: CAT II) The IAO will ensure all e-mail security related software patches are applied and documented.*

- *(DTMG002: CAT II) The IAO will ensure the latest maintenance rollup or service packs for the e-mail client are applied and documented.*

NOTE: Generally a couple of months will be allowed for any problems to be reported to the vendor prior to new maintenance rollup or service packs being required.

SAs and IAOs should regularly check email vendor web sites for information concerning products or versions of products no longer being supported. Action should be taken to ensure a smooth migration plan is developed and implemented prior to a product going into a nonsupport status.

- *(DTMG003: CAT I) The IAO will ensure unsupported e-mail software is removed or upgraded prior to a vendor dropping support.*

- *(DTMG004: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading e-mail software prior to the date the vendor drops security patch support.*

6.2 General Guidance for E-mail Clients

Some e-mail clients enable technologies that support the execution of mobile code and utilize PKI technologies to support some features

- *(DTMG005: CAT II) The SA will ensure e-mail clients used to connect to Government servers support digital signature and encryption services.*

NOTE: This support will be compatible with the DoD PKI.
As described previously, attachments containing malicious code are a common method of attacking using an e-mail client.

- *(DTMG006: CAT II) The SA will ensure e-mail clients disable the automatic opening of e-mail attachments that may contain mobile code in the e-mail body and attachments.*

- *(DTMG007: CAT II) The SA will ensure e-mail clients prompt before opening of e-mail attachments that may contain mobile code in the e-mail body and attachments.*

NOTE: It must be recognized that these features do not remove the danger from malicious attachments. If a user saves the file to disk, the malicious code remains. Thus, the feature is not a substitute for an anti-virus tool with current definitions.

E-mail in HTML format can contain malicious mobile code. In order to prevent mobile code from executing by opening an e-mail, the e-mail client can be configured to read the file as text.

- *(DTMG008: CAT II) The SA will ensure e-mail clients are configured to read HTML content as text and disable the viewing of HTML attachments inline.*

This page is intentionally left blank.

7. OFFICE AUTOMATION SUITES

Office automation suites are collections of programs that support common tasks. A standard suite often includes word processing, spreadsheet, and presentation applications. A professional or premium suite usually adds some form of data base management system. The popularity of office automation products, coupled with strong programming interfaces, makes them attractive targets for people with malicious intent.

One common form of attack exploits the macro capability that is offered in some office automation applications. Macros are a form of mobile code (e.g., VBA macros, PerfectScript macros) and can be used maliciously. Features that support automatic macro invocation when a document is opened are prime targets for virus authors. Other attacks may exploit vulnerabilities associated with new features that support HTML or other mobile code technologies such as Microsoft's ActiveX. Additionally, office automation files may also contain embedded ActiveX controls. Because office automation files become mobile code when downloaded via e-mail or from a web site, the automatic execution of mobile code in office automation files must be constrained in accordance with the DoD Mobile Code Policy.

The following sections provide general guidance that applies to all office automation suites. It defines the principles that are applied in the product-specific requirements that are described in Appendix E. If there is a requirement to use software that is not covered in Appendix E, the guidance in this section must be applied.

7.1 Software Maintenance

Maintaining the security of office automation products requires frequent reviews of security bulletins. Many security bulletins mandate the installation of a software patch to overcome security vulnerabilities.

SAs and IAOs should regularly check vendor web sites for information on new security patches that are applicable to their site. All applicable security patches will be applied to the system. A security patch is deemed applicable if the product is installed, even if it is not used or is disabled.

FSO does not test or approve patches or service packs. It is the site's responsibility to test vendor patches within their test environment.

- *(DTOG001: CAT II) The IAO will ensure all office automation security related software patches are applied and documented.*

- *(DTOG002: CAT II) The IAO will ensure the latest maintenance rollup or service packs for the office automation product are applied and documented.*

NOTE: Generally a couple of months will be allowed for any problems to be reported to the vendor prior to new maintenance rollup or service packs being required.

SAs and IAOs should regularly check office automation product vendor web sites for information concerning products or versions of products no longer being supported. Action should be taken to ensure a smooth migration plan is developed and implemented prior to a product going into a nonsupport status.

- *(DTOG003: CAT I) The IAO will ensure unsupported office automation software is removed or upgraded prior to a vendor dropping support.*

- *(DTOG004: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading office automation software prior to the date the vendor drops security patch support.*

7.2 General Guidance for Office Automation Suites

- *(DTOG005: CAT II) The SA will ensure document password features are not used to provide file security unless it can be determined there is adequate encryption or other protection of the password.*

- *(DTOG006: CAT II) The SA will ensure the office automation product is configured to disable (or prompt) the user prior to the execution of embedded macros.*

NOTE: This is particularly important for macros that are invoked automatically when a host document is opened.

8. ANTISPYWARE

Spyware is any software that covertly gathers information about a user without his or her knowledge and transmits this data to a third party through an Internet connection. Many times the term is associated with adware. Adware is software that presents a user with advertising messages based on an analysis of collected data to determine the types of items or services that may be of interest to the user. Many times the terms are used together in the context of adware/spyware because adware sometimes collects data to better target the user with the types of ads to present. The security concern of this type software lies with the data transmission that is unknown to the user. The best way to avoid a spyware infection is to limit Internet browsing to non-admin accounts and follow the configuration guidance in this document for web browsers.

Even with all the layers of protection in place, this type of software is becoming more of an issue. In addition to preventing the installation of this type of software, monitoring for its existence is extremely important. This is accomplished through the installation of an AntiSpyware program. Many of these programs have the capability to configure a machine to prevent an attack, as well as scan for and remove the malicious code. In order for a program to be effective it must be used to regularly scan the machine, it must protect the machine real time while connected to a network, and in the case that the user suspects there is an issue, the program must provide an on-demand capability for detection.

- *(DTSG001: CAT I) The SA will ensure every machine has an AntiSpyware program installed and active for on-access and on-demand AntiSpyware detection.*

The following sections provide general guidance that applies to all AntiSpyware software.

8.1 Software Maintenance

- *(DTSG002: CAT I) The SA will ensure the AntiSpyware software installation is a supported version.*

- *(DTBG003: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading antispyware software prior to the date the vendor drops security patch support.*

- *(DTSG004: CAT II) The SA will ensure the latest maintenance rollup or software update for the AntiSpyware software is applied.*

- *(DTSG005: CAT II) The SA will ensure AntiSpyware software installation and update files are only downloaded from a trusted site such as the JTF-GNO NetDefense, DoD Download Server Service, or directly from the vendor's site.*

- *(DTSG006: CAT II) The SA will ensure antisypware definition/signature files are automatically updated at least weekly.*

NOTE: It is recommended the signatures be updated daily.

- *(DTSG007: CAT I) The SA will ensure signature files are no older than 14 days.*

- *(DTSG008: CAT II) The SA will ensure Beta or non-production versions of definition/signature files are not used on production machines.*

8.2 General Guidance for AntiSpyware Software

This section details general guidance for the configurations of AntiSpyware products.

- *(DTSG009: CAT II) The SA will ensure AntiSpyware software is configured to start on-access protection automatically when the machine is booted.*

- *(DTSG010: CAT II) The SA will ensure AntiSpyware software is configured to perform a scan of the local hard drives at least weekly.*

NOTE: Scans at boot time (or daily) are recommended when this would not cause a significant impact to operations.

- *(DTSG011: CAT II) The SA will ensure the AntiSpyware software, when running a scheduled scan, is configured to scan memory and drives (including a deep or in depth scanning option).*

In the event that potentially malicious activity or a potentially malicious program is found, the user must be notified. This allows the user to take any additional action to reduce damage and halt propagation of the potential damage. The user should also exercise the appropriate computer security incident reporting requirements as defined by the site.

- *(DTSG012: CAT II) The SA will ensure the AntiSpyware software, when running in on-access mode, is configured to inform the user at the time potentially malicious activity is detected.*

- *(DTSG013: CAT II) The SA will ensure the AntiSpyware software, when running in scheduled mode, is configured to inform the user at the time potentially malicious activity is detected.*

- *(DTSG014: CAT II) The SA will ensure the AntiSpyware software, when running in on-demand mode, is configured to inform the user at the time potentially malicious activity is detected.*

- *(DTSG015: CAT III) The SA will ensure the AntiSpyware software is configured to maintain AntiSpyware log files for at least 30 days.*

- *(DTSG016: CAT III) The SA will ensure the AntiSpyware log files are reviewed.*

- *(DTSG017: CAT III) The IAO will ensure an incident response procedure exists which provides detailed procedures for the user when a suspected infection occurs or when the software generates a warning.*

This page is intentionally left blank.

9. SECURING REMOTE AND MOBILE ACCESS DEVICES

Although users of desktop applications are usually connected to, and protected by, a network that is part of a secure enclave, there are cases where a user may use alternate network connections or mobile devices for processing DoD sensitive information. Remote and mobile devices present a risk to the DoD network because these devices are frequently lost, stolen, or have disabled or outdated security protection mechanisms.

Remote devices connect are devices that are not directly connected to the Enclave and use alternate connection methods such as broadband, dial-up, or wireless connections to access the network. Mobile devices can connect remotely using dial-up or wired infrastructure; use wireless protocols to connect remotely; or connect directly to the network using wireless network; or connect to a PC which itself is connected to the Enclave. Mobile devices include laptops, handheld computers, and Portable Electronic Devices (PEDs). PEDs include BlackBerry devices, personal digital assistants (PDAs), palmtops, handheld computers, cellular phones, two-way pagers, wireless keyboards and mice. The following sections detail requirements for remote PCs and mobile devices to connect remotely to network resources or use alternate network connections. Security policy requirements for PEDs and wireless mobile devices are located in the Wireless Security STIG.

9.1 Remote Access Devices

Remote access from any location is considered untrusted. Whether the method consists of dialing into a Remote Access Server or using a form of broadband technology, the following general guidelines must be followed for securing remote devices, to include but not limited to laptops, workstations, and PEDs. The requirements in the following subsections will be met for Administrative Access and to the fullest extent possible for End-User and Limited Access.

- *(SRC191: CAT II) The SA will ensure if a modem is present, in-coming dial-up capability to the user's remote device (e.g., laptop, workstation, PEDs, etc.) is disabled.*

- *(SRC192: CAT III) The SA will ensure all remote access devices are configured so that the operation of the NIC and the modem is mutually exclusive (i.e., using hardware profiles, if the NIC is initialized, then the modem is disabled).*

- *(SRC360: CAT III) The IAO will ensure no changes to the security configuration of software or hardware of a Government controlled remote access device are made without prior approval of the IAO.*

- *(SRC361: CAT III) The IAO will ensure there is a mechanism in place to scan a remote access device for viruses, immediately upon connection to a DoD network when the remote user returns to their official duty station.*

The risk of exposure to vulnerabilities, malicious attackers, and opportunistic individuals is significantly increased with the use of "always–on" technologies such as broadband. Users are connected for much longer periods and these connections often use static IP addresses provided

by Internet Service Providers (ISP), providing a "fixed" target for the attacker. Furthermore, the additional speed and bandwidth of the connection makes it an attractive alternative over dial-up to not only the remote user, but the attacker as well. The threat of attack is the same for broadband communication as it is for any Local Area Network (LAN). Because of its open architecture, connections to the Internet are inherently vulnerable and are subject to scans, probes, worms, Trojans, denial of service, spoofing, Zombies, etc. Therefore, it is imperative that any broadband connection be as secure as possible prior to connecting to a DoD network or resource.

Although the risks are greater with high-speed connections than with dial-up, those risks can be minimized with security measures such as personal firewalls, web browser security settings, operating system secure configurations, anti-virus software with updated signature files, and encryption.

- *(SRC190: CAT II) The IAO will ensure file and print sharing is disabled on remote access devices, as there is an inherent risk associated with the technologies employed by broadband architectures.*

NOTE: If **File and Print Sharing** is enabled this requirement can be met by a personal firewall policy filtering inbound 445.

9.2 Personal Firewalls

Attackers are constantly scanning and probing the Internet and associated IP addresses for known vulnerabilities. Although it is a requirement that some Government agencies install and configure firewalls to minimize the threat to internal systems, not all agencies have been able to implement firewall architectures. Therefore, in an effort to mitigate attacks on DoD systems and thwart the efforts of attackers, personal firewalls are required on remote access devices. Personal firewalls create an additional defense mechanism and help minimize Distributed Denial of Service (DDoS) attacks, where numerous compromised systems attack a single target, thereby creating a denial of service for legitimate users of that targeted system. Firewalls also help to prevent Trojans, hijacking of data, and the introduction of "backdoors" into a system.

- *(SRC1630: CAT II) The IAO will ensure any device that accesses a DoD network remotely has a personal firewall installed.*

NOTE: This includes all devices that are capable of dialing in via modem.

NOTE: Products from the DoD standard contract should be used.

NOTE: Use of Personal Firewalls on DoD enclave workstations, if not centrally-managed, may result in the inability for organizational security staff to remotely scan those workstations effectively for vulnerabilities.

- *(SRC1631: CAT III) The IAO will ensure the site has developed a configuration baseline and policy regarding the use and configuration of personal firewalls for remote access clients.*

- *(SRC410: CAT I) The IAO will ensure all known DDoS ports and NetBIOS ports are bi-directionally blocked by the personal firewall. Refer to the Network Infrastructure STIG, and the DoD Ports, Protocols, and Services (PPS) Assurance Category Assignments List for detailed port blocking guidance.*

- *(SRC400: CAT I) The IAO will ensure all outgoing packets, except those necessary for operation (e.g., SMTP, SSL, HTTP, HTTPS, FTP, etc.) are blocked at the personal firewall. Refer to the Network Infrastructure STIG for port blocking guidance. Allowable protocols are documented.*

- *(SRC405: CAT II) The IAO will ensure the firewall is configured to block Category 1X and unsigned Category 1A mobile code, if technically feasible.*

- *(SRC420: CAT II) The IAO will ensure a "deny by default" posture is enforced on personal firewalls. The IAO will ensure only ports or services required for operational use are open on the firewall and that all open ports are documented.*

- *(SRC430: CAT III) The NSO/IAO will ensure the personal firewall is configured to log all inbound connections.*

- *(SRC440: CAT III) The IAO will ensure the firewall logs are reviewed at least weekly and unusual events or suspicious activity is reported to the security officer.*

- *(SRC450: CAT II) The IAO will ensure the personal firewall is configured at a minimum to a "Medium" level of security to include the following:*

  - *Blocking all Internet access until expressly permitted by the user*
  - *Silently block unused ports*
  - *Prompt for Java Applet and ActiveX controls*

- *(SRC451: CAT III) The IAO will ensure the personal firewall is configured to alarm the user for all suspicious events or intrusions.*

- *(SRC452: CAT III) The IAO will ensure if the capability exists within the firewall software to report errors back to the vendor, the messages are either redirected to the DoD site for review by the NSO, or disabled.*

9.3 Passwords on Remote Access Devices

Password cracking and brute force software packages, such as John the Ripper or THC-Hydra, are widely available on the Internet. The first line of defense against attack of any computer system is a strong, unique, hard to crack password. All remote access devices, regardless of technology, must be password protected.

- *(SRC1561: CAT II) The IAO will ensure accepted password generation schemes to create passwords are used. At a minimum, passwords are created and maintained (i.e., they are changed) in accordance with the rules outlined in CJCSM 6510 policy established in the DoDI 8500.2.*

- *(SRC1562: CAT II) The IAO will ensure a schedule is in place to periodically (at least every 180 days) check passwords using password-cracking software.*

9.4 Encryption and Authentication

Encryption, although not a secure solution alone, is a powerful tool used to secure the privacy and integrity of data. There are two primary forms of encryption—asymmetric and symmetric. Public key encryption is a cryptographic asymmetric system that uses two keys—public to encrypt the data, and private to decrypt the data. Private Key or symmetric encryption, utilizes only one secret key to perform the encryption and decryption process. If a device, PC, or laptop is lost or stolen, it is important that the Government data contained on the device be as secure as possible to avoid compromise. The best means of protecting data on mobile devices is by encrypting the files on the device itself. These requirements apply to all mobile devices used to process, store, or connect to DoD sensitive information or resources, regardless of the connectivity configuration. This includes laptops, PEDs, USB devices, etc.

- *(SRC570: CAT II) The IAO will ensure the remote user employs a FIPS 140-2 approved file encryption algorithm (i.e., AES, 3DES) to encrypt all Government data on the mobile device unless the data is determined to be non-sensitive by the Deputy Secretary of the Service or Agency.*

- *(SRC590: CAT II) The IAO will ensure remote users back up and store the private encryption key in a secure location (e.g., floppy disk, CD, etc.).*

- *(SRC600: CAT III) The IAO will ensure there is a mechanism in place for key recovery or data recovery to prevent loss of data if the user losses the encryption key.*

Authentication for Windows based machines is usually based on a domain structure. With so many devices now being mobile, additional considerations also need to be given for authentication of the mobile device for remote and local access.

- *(SRC605: CAT II) The IAO will ensure the timeout for re-authentication on remote and mobile devices is 30 minutes or less.*

- *(SRC606: CAT II) The IAO will ensure remote access authentication is based on two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.*

9.5 VPN Client

For a remote access VPN to be as secure as possible, the traffic must be both encrypted and integrity protected. That is to say, without encryption, an unauthorized person could access the data, and without integrity protection, encrypted traffic is susceptible to attacks and modification of data. The VPN client software communicates with a VPN device within the network infrastructure and establishes a secure connection over the Internet. It is strongly recommended that with any implemented VPN solution the VPN client should be from the same vendor.

- *(SRC1800: CAT II) The remote user will ensure Split Tunneling is disabled on the VPN Client (i.e., upon the establishment of a VPN connection to a DoD network, no other connections of any kind are established [e.g., if home networks are used, no connection between the device and other home network devices are established during a VPN session]).*

- *(SRC610: CAT II) The remote access user will not configure or change security settings of the VPN client without prior approval from the system or network administrator.*

- *(SRC620: CAT III) The IAO will ensure the remote user has complete instructions on the use of a VPN client used to access a DoD network or resource.*

- *(SRC630: CAT II) The IAO will ensure a VPN client supports and is configured for IPSec attributes such as 3DES, Tunnel encapsulation mode, and a FIPS 140-2 validated encryption algorithm.*

.

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

Government Publications

Department of Defense, Chief Information Officer Memorandum, "Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems," 23 October 2006.

Department of Defense Instruction, "Department of Defense (DoD) Public Key Infrastructure (PKI) and Public Key (PK) Enabling", 1 April 2004.

Department of Defense, DoD Directive (DoDD) 8500.1, "Information Assurance (IA)," October 24, 2002.

Department of Defense, "X.509 Certificate Policy for the United States Department of Defense," Version 5.2, 13 November 2000.

Defense Information Systems Agency, "Secure Remote Computing Security Technical Implementation Guide".

Executive Office of the President, Office of Management and Budget Memorandum, "Protection of Sensitive Agency Information", 23 June 2006.

National Security Agency (NSA), "E-mail Security in the Wake of Recent Malicious Code Incidents," Version 2.6, 29 January 2002.

National Security Agency (NSA), "Microsoft Office 2000 Executable Content Security Risks and Countermeasures," 8 February 2002.

National Security Agency (NSA), "Microsoft Office XP/2003 Executable Content Security Risks and Countermeasures," 10 February 2005.

Government Web Sites

http://www.disa.mil/	Defense Information Systems Agency
https://datahouse.disa.mil/	Defense Information Systems Agency Datahouse
http://iase.disa.mil/ (NIPRNet)	Defense Information Systems Agency Information Assurance Support Environment
https://www.jtfgno.milhttp://www.cert.mil/ (NIPRNet)	JTF-GNO NetDefense
http://dodpki.c3pki.chamb.disa.mil/ or http://dodpki.c3pki.den.disa.mil/	Department of Defense Class 3 Public Key Infrastructure (PKI) Home Page
http://www.c3i.osd.mil/org/sio/ia/pki.html	Department of Defense Public Key Infrastructure Program Management Office(DoD PKI PMO)
http://www.nsa.gov/isso/index.html	National Security Agency Information Assurance Directorate (NSA IAD)

Commercial and Other Non-government Sites

http://www.icsalabs.com/	International Computer Security Association (ICSA) Labs
http://www.mozilla.org	FireFox Information
http://www.mcafee.com/support/	McAfee Support
http://www.microsoft.com/downloads/search.asp	Microsoft Download Center
http://www.microsoft.com/windows/ie/downloads/default.asp	Microsoft IE Product Downloads
http://www.microsoft.com/technet/security/current.asp	Microsoft TechNet Security
http://channels.netscape.com/ns/browsers/default.jsp	Netscape Browser Central
http://wp.netscape.com/security/notes/index.html	Netscape Security Notes
http://www.symantec.com/techsupp/	Symantec Service & Support
http://www.wildlist.org/	The WildList Organization

APPENDIX B. ANTIVIRUS PRODUCT SPECIFIC GUIDANCE

The JTF-GNO NetDefense makes several anti-virus tools available for download from their web site at https://www.jtfgno.mil/antivirus/av_info.htm. These tools include two familiar anti-virus client packages that can be used for machines running Windows 2003, 2000, or XP:

- Symantec Norton AntiVirus Corporate Edition
- McAfee VirusScan

B.1 Symantec AntiVirus Corporate Edition Version 9.x/10.x

Symantec's AntiVirus Corporate Edition, known hereafter as AntiVirus CE, provides protection from viruses that spread from hard drives, floppy disks, e-mail attachments, and other files that travel across networks. Symantec AntiVirus CE can be used for stand-alone protection or as a managed client that is attached to a Symantec AntiVirus server. This document provides guidance based on a stand-alone implementation.

The following installation considerations should be noted:

- Options for the protection of e-mail clients (Microsoft Exchange/Outlook and Lotus Notes) may be displayed during installation. Therefore e-mail clients should be configured before Symantec AntiVirus CE is installed.

- An option to enable File System Auto-Protect at Windows startup is displayed during installation. If this option is enabled at installation, later configuration tasks are a bit easier.

The configuration guidelines for Symantec AntiVirus CE are divided into the following sections:

- Software Maintenance
- Symantec AntiVirus Services
- Auto-Protect
- History Options
- Schedule Virus Definition Updates
- Scheduled Scans or Startup Scans.

B.1.1 Software Maintenance

NOTE: All patching and product support requirements (DTAG002-DTAG003) as detailed in *Section 4.1, Software Maintenance*, apply to Symantec AntiVirus CE.

B.1.2 Symantec AntiVirus Startup

- *(DTAS001: CAT II) The SA will ensure the Symantec AntiVirus Auto-protect is configured to start at system startup.*

- *(DTAS002: CAT II) The SA will ensure the Symantec AntiVirus Services are configured to make certain that changes that require the software to restart automatically occur.*

These settings are controlled from the Symantec Antivirus, Configure, File System Auto-protect, Advanced tab.

B.1.3 Auto-Protect

- *(DTAS003-DTAS017, DTAS060-DTAS074: CAT II) The SA will ensure the File System Auto-Protect parameters are configured according to the settings in the following table:*

FILE SYSTEM AUTO-PROTECT PROTECTION SETTINGS		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
File System Auto-Protect	*Enable file system Auto-Protect File types:* *- All types* *- Selected* *Options:* *- Display message on infected computer (9.x)* *- Exclude selected files and folders* *Macro Virus (Version 9.x)* *- 1. Action:* *- 2. If action fails:* *Non-Macro Virus (Version 9.x)* *- 1. Action:* *- 2. If action fails:* *Version 10.x* *-Block Security Risks* *-Scan for Security Risks* *-For Leave Alone (Log Only)* *Delete infected files on creation* *Threat Tracer* *-Enable Threat Tracer*	 *Enable* *Disable* *Enable* *Disable* *Clean virus from fileQuarantine infected file* *Clean virus from file* *Quarantine infected file* *Enable* *Enable* *Enable* *Enable*
File System Advanced Options	*Auto-Protect will scan files that are:* *- Accessed or modified (scan on create, open, …)* *Backup options:* *- Back up file before attempting repair*	 *Enable* *Enable*

FILE SYSTEM AUTO-PROTECT PROTECTION SETTINGS		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
	Automatic Enabler *-When Auto-Protect is disabled, enable after [value] minutes*	*5 or less*
Check Floppies	*Floppy settings:* *- Check floppies for boot viruses upon access* *- When a boot virus is found:* *System shutdown settings:* *- Do not check floppies upon system shutdown*	*Enable* *Clean virus from boot record* *Disable*
Heuristics (Version 10.x only)	*Enable Bloodhound virus detection technology* *Desired level*	*Enabled* *Default or Maximum (Note Maximum may have undesirable operational effects)*
Actions (Version 10.x)	*Macro Virus – First Action* *Macro Virus – Second Action* *Non- Macro Virus – First Action* *Non- Macro Virus – Second Action* *Security Risks – First Action* *Security Risks – Second Action* *(Note: Any sublevels that override the higher level will not be configured as Leave Alone)*	*Any action except Leave Alone* *Any action except Leave Alone* *Any action except Leave Alone* *Any action except Leave Alone* *Any action except Leave Alone* *Any action except Leave Alone*

Table B-1. File System Auto-Protect Settings

These settings can be configured in the Configure | File System Auto-Protect dialog of the Symantec AntiVirus Corporate Edition application.

Symantec AntiVirus CE can be configured for interaction with three mail programs:

- Internet Mail
- Lotus Notes
- Exchange (an Outlook client)

Symantec AntiVirus CE will be configured to interact with the mail client installed. The following requirements use Exchange as an example. The requirements will be applied to the installed mail program

- *(DTAS020-DTAS029, DTAS80-DTAS086: CAT II) The SA will ensure the parameters are configured according to the settings in the following table for the installed mail client:*

EMAIL AUTO-PROTECT SETTINGS		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
[Mail Client] Auto-Protect	*Enable {Mail Client] Auto-Protect* *File types:* *- All types* *- Selected Extensions* *- Selected Types* *Notifications: (Version 9.x)* *- Display message on infected computer* *- Insert warning into e-mail message* *Macro Virus* *- 1. Action:* *- 2. If action fails:* *Non-Macro Virus* *- 1. Action:* *- 2. If action fails:* *Email Messages (Version10.x)* *- Insert warning into e-mail message*	 *Enable* *Enable* *[see note following table]* *Disable* *Disable* *Enable* *Enable* *Clean virus from file* *Quarantine infected file* *Clean virus from file* *Quarantine infected file* *Enable*
Advanced Options	*When scanning compressed files:* *- Scan files inside compressed files*	 *Enable*

EMAIL AUTO-PROTECT SETTINGS		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
Actions (Version 10.x)	*Macro Virus – First Action*	*Any action except Leave Alone*
	Macro Virus – Second Action	*Any action except Leave Alone*
	Non- Macro Virus – First Action	*Any action except Leave Alone*
	Non- Macro Virus – Second Action	*Any action except Leave Alone*
	Security Risks – First Action	*Any action except Leave Alone*
	Security Risks – Second Action *(Note: Any sublevels that override the higher level will not be configured as Leave Alone)*	*Any action except Leave Alone*

Table B-2. Mail Client Auto-Protect Settings

NOTE: Setting the Auto-Protect file types parameter to a value other than "All types" is appropriate only in environments that are categorized to be low risk. In addition, a written Antivirus plan must be in place with the IAO indicating this type of checking is being performed by the mail server.

These settings can be configured in the Configure | [Choose the appropriate mail client] dialog of the Symantec AntiVirus Corporate Edition application.

B.1.4 History Options

- *(DTAS030: CAT II) The SA will ensure the History Options parameter is configured so history is maintained for at least 30 days.*

This setting can be configured in the File | Configure Histories dialog of the Symantec AntiVirus Corporate Edition application.

B.1.5 Schedule Virus Definition Updates

- *(DTAS031: CAT II) The SA will ensure the virus updates are configured to automatically update at least weekly.*

NOTE: It is recommended that this feature be configured to run daily.

This setting can be configured through the File | Schedule Updates dialog of the Symantec AntiVirus Corporate Edition application.

B.1.6 Scheduled Scans or Startup Scans

To supplement the safeguard provided by the Auto-Protect features, it is necessary to have a periodic virus scan of the machine's local hard drive(s) on at least a weekly basis. This can be accomplished by defining a task to Scheduled Scans or to Startup Scans.

The difference between a Scheduled Scans task and a Startup Scans task is the time at which the scan is performed. A Scheduled Scans task is performed at a specific, configured time. A Startup Scans task is performed when the machine is booted.

A schedule scan can be created initially using the Edit | New Scheduled Scan or Edit | New Startup Scan dialog of the Symantec AntiVirus Corporate Edition application.

Specific parameters are required to ensure that either type of task is configured and scheduled properly.

- *(DTAS032: CAT II) The SA will ensure either a Startup Scans task exists or a Scheduled Scans task is configured to perform a virus scan of the machines's local drive(s) at least weekly.*

- *(DTAS037-DTAS050, DTAS090-DTAS099: CAT II) The SA will ensure the Scheduled Scans task or Startup Scans task is configured according to the settings in the following table:*

SCHEDULED SCANS \ STARTUP SCANS FILES SETTINGS		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
Scan	*Files*	*[- All local hard drivers must be selected. - All folders and files must be selected.]*

SCHEDULED SCANS \ STARTUP SCANS FILES SETTINGS		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
Scan Options	*File types:* *- All types*	*Enable*
	- Selected Extensions	*Disable*
	- Selected Types	*Disable*
	Options: (Version 9.x)	
	-Scan for in memory enabled	*Enable*
	-Scan for extended threats	*Enable [Recommended]*
	- Display message on infected computer	*Enable*
	- Exclude files and folders (Version 9.x and 10.x)	*Disable*
	Macro Virus (Version 9.x)	*Clean virus from file*
	- 1. Action:	*Quarantine infected file*
	- 2. If action fails:	*Clean virus from file*
	Non-Macro Virus (Version 9.x)	*Quarantine infected file*
	- 1. Action:	
	- 2. If action fails:	
	Version 10.x *Scan Enhancements:* *-Scanning program files loaded into memory*	*Enable*
	-Scanning common infection locations (load points)	*Enable*
	-Scanning for traces of well-known viruses and Security risks before scanning selected files and folders	*Enable*

SCHEDULED SCANS \ STARTUP SCANS FILES SETTINGS		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
Scan Advanced Options	*When scanning compressed files:* *- Scan files inside compressed files*	*Enable*
	Backup options: *- Back up file before attempting repair*	*Enable*
	Dialog options: *- Show scan progress*	*Enable*
	-Allow user to stop scan	*Disable*
Actions (Version 10.x)	*Macro Virus – First Action*	*Any action except Leave Alone*
	Macro Virus – Second Action	*Any action except Leave Alone*
	Non- Macro Virus – First Action	*Any action except Leave Alone*
	Non- Macro Virus – Second Action	*Any action except Leave Alone*
	Security Risks – First Action	*Any action except Leave Alone*
	Security Risks – Second Action *(Note: Any sublevels that override the higher level will not be configured as Leave Alone)*	*Any action except Leave Alone*

Table B-3. Scheduled Scans \ Startup Scans Files Settings

B.1.7 Tamper Protection (Version 10.x)

Version 10.x provides the ability for protection of antivirus processes to be tampered with. This is controlled through the Tamper Protection dialog under Configure.

- *(DTAS110: CAT II) The SA will ensure the 'Tamper Protection' option is enabled.*

- *(DTAS111: CAT II) The SA will ensure the 'Tamper Protection' is set to'Block if a violation is found'.*

- *(DTAS112: CAT II) The SA will ensure the 'Tamper Protection' option is enabled even if antivirus is shutdown.*

- *(DTAS113: CAT II) The SA will ensure the 'Tamper Protection' option to display a message to the user is enabled.*

B.2 McAfee VirusScan Enterprise 7.x/8.x

Network Associates Inc.'s McAfee VirusScan provides a comprehensive anti-virus solution for clients. It includes on-access scanning, on-demand scanning, and task scheduling.

The following installation considerations should be noted:

- The IAO should evaluate the "Security Type" option. The "Maximum Security" value restricts non-administrative users from changing some sensitive configuration options. However, in software development environments, the "Standard Security" value may be more practical.

- The E-mail Scan, Download Scan, and Internet Filter options may not, depending on the release of the product, be part of the "Typical" setup. A "Custom" setup may be required to obtain these components during initial product installation. If not installed initially with the product, the components can be added later.

The configuration guidelines for VirusScan are divided into the following sections:

- Software Maintenance
- On Access Scan
- AutoUpdate
- Email Scan
- Scheduled Scans

B.2.1 Software Maintenance

NOTE: All patching and product support requirements (DTAG002-DTAG003) as detailed in *Section 4.1, Software Maintenance,* apply to VirusScan.

B.2.2 On-Access Scan

The following items can be configured from the Task | On-Access Scan Properties Dialog.

- *(DTAM001: CAT II) The SA will ensure the 'On-Access Scan' is enabled.*

- *(DTAM002-DTAM014, DTAM090-DTAM117: CAT II) The SA will ensure the On-Access parameters are configured to the following requirements:*

VSHIELD SYSTEM SCAN SETTINGS		
TAB NAME	***PARAMETER***	***REQUIRED SETTING***
General	*Scan* *-Boot sectors* *-Floppy during shutdown*	 *Enable* *Enable*
Script Scan (Version 8.x only)	*- Enable Script Scan*	*Enable*
Blocking (Version 8.x only)	*- Block the Connection* *- Unblock after (minutes)* *- Block if an unwanted program is detected*	*Enabled* *30* *Enabled*
Messages	*Messages for local users:* *-Show the message dialog when a virus is detected* *Non-Admin actions:* *- Remove messages from the list* *- Clean infected files* *- Delete infected files* *- Move infected files to the quarantine folder*	 *Enable* *Disable* *Enable* *Enable* *Enable*
Reports	*Log File:* *- Log to file* *- Limit size of log file to kilobytes* *What to log:* *- Session settings* *- Session summary* *- Failure to scan encrypted files* *- User name*	 *Enable* *Enable* *100* [or higher] *Enable* *Enable* *Enable* *Enable*

VSHIELD SYSTEM SCAN SETTINGS		
TAB NAME	***PARAMETER***	***REQUIRED SETTING***
Processes	*- Use Settings on these tabs for all processes*	*Enabled*
Detection	*- Scan files when writing to disk* *- Scan files when reading from disk* *- Scan all files*	*Enabled* *Enabled* *Enabled*
Advanced	*- Heuristics – Find unknown program viruses* *- Heuristics – Find unknown program viruses* *- Scan inside archives* *- Decode MIME encoded files*	*Enabled* *Enabled* *Enabled* *Enabled*
Actions	*-Primary Action* *-Secondary Action*	*Any action except allow access to file* *Any action except allow access to file*
Unwanted Programs	*-Detect unwanted Programs* *-Primary Action* *-Secondary Action*	*Enabled* *Any action except allow access to file* *Any action except allow access to file*

Table B-4. On-Access Scan Settings

B.2.3 AutoUpdate

The VirusScan can be configured to allow automatic updates of signature files by double clicking on the "AutoUpdate Task" from the VirusScan console.

- *(DTAM016: CAT II) The SA will ensure VirusScan is configured to use the 'AutoUpdate' feature at least weekly.*

- *DTAM017: CAT II) The SA will ensure VirusScan is configured to get newer definition files, if available.*

- *DTAM018: CAT II) The SA will ensure VirusScan is configured to get newer detection engines, if available.*

- *DTAM019: CAT II) The SA will ensure VirusScan is configured to get other available updates.*

NOTE: It is recommended that the AutoUpdate feature be configured to run daily.

B.2.4 E-Mail Scan

The following items can be configured from the Task | E-mail scan| Properties dialog.

- *(DTAM021-DTAM041: CAT II) The SA will ensure the VirusScan E-mail Scan parameters are configured according to the settings in the following table:*

VIRUSSCAN E-MAIL SCAN SETTINGS		
TAB	***PARAMETER***	***REQUIRED SETTING***
Detection	*Enable Microsoft Exchange Attachments:* *- All attachments*	*Enable* *Enable*

VIRUSSCAN E-MAIL SCAN SETTINGS		
TAB	***PARAMETER***	***REQUIRED SETTING***
Advanced	*Heuristics* *-Find unknown program viruses* *-Find unknown macro viruses* *Non-viruses* *-Find potentially unwanted programs (Version 7.x only)* *-Find attachments with multiple extensions* *Compressed Files* *-Scan inside packed executables (Version 7.x only)* *-Scan inside archives* *-Decode MIME encoded files* *E-mail message body* *-Scan email message body*	 *Enable* *Enable* *Enable [Recommended]* *Enabled [Recommended]* *Enabled* *Enabled* *Enabled* *Enabled*
Action	*When a virus is found* *Possible Actions:* *-Clean file* *-Delete Attachment* *-Move Attachment*	*Prompt for action* *Enable* *Enable* *Enable*
Alerts	*Email alert* *-Return reply to sender* *If 'Prompt for Action' is selected:* *-Display custom message*	 *Enable* *Appropriate user message*

VIRUSSCAN E-MAIL SCAN SETTINGS		
TAB	***PARAMETER***	***REQUIRED SETTING***
Reports	*Log File:* *- Log to file* *- Limit size of log file to* *- kilobytes* *What to log:* *- Session settings* *- Session summary* *- Date and Time* *-User Name* *-Failure to scan encrypted files*	 *Enable* *Enable* *100* [or higher] *Enable* *Enable* *Enable* *Enable* *Enable*
Detect Unwanted Program (Version 8.x only)	*- Detect unwanted programs* *- Primary Action*	*Enabled* *Prompt for Action*

Table B-5. Virusscan E-Mail Scan Settings

B.2.5 Scan All Fixed Disks

The Scan All Fixed Disks properties provide task management of scanning and scheduling services.

Creating a task and scheduling it at least weekly with the following parameters is required.

- *(DTAM045-DTAM066: CAT II) The SA will ensure a scan is configured to perform a virus scan of the machine's local drive(s), using the following settings:*

SCAN SETTINGS FOR SCAN		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
Where	*Item to be scanned* *Scan Options* *-Include subfolders* *-Scan boot sectors*	*All Fixed Disks* *Memory of running processes* *Enable* *Enable*

SCAN SETTINGS FOR SCAN		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
Detection	*What to scan:* *- All files* *- User specified files* *What not to scan* *- Exclusions* *Compressed files* *-Scan inside packed executables* *-Scan inside of archives* *-Decode MIME encoded files*	 *Enable* *Enable* *None* *Enabled* *Enabled* *Enabled*
Advanced	*Heuristics* *-Find unknown program viruses* *-Find unknown macro viruses* *Non-viruses* *-Find potentially unwanted programs (Version 7.x only)*	 *Enable* *Enable* *Enable [Recommended]*
Action	*When a virus is found* *If action fails* *Folder Name*	*Clean infected files automatically* *Move infected files to a folder* *Quarantine*
Unwanted Programs (Version 8.x only)	*Detect Unwanted programs*	*Enabled*

SCAN SETTINGS FOR SCAN		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
Report	*Log File:* *- Log to file* *- Limit size of log file to kilobytes* *What to log:* *- Session settings* *- Session summary* *- Failure to scan encrypted files* *- User name*	 *Enable* *Enable* *100* [or higher] *Enable* *Enable* *Enable* *Enable*

Table B-6. Scan Settings for Scan

- *(DTAM070: CAT II) The SA will ensure a scan is configured to automatically execute and is performed at least weekly.*

This can be scheduled by selecting the Schedule Option from the Scan Properties, then selecting the Enable option from the schedule settings on the Task tab. The frequency of the scan can then be configured from the schedule tab.

B.2.6 Buffer Overflow Protection (Version 8.x only)

The Buffer Overflows dialog controls if the product will protect against buffer overflows.

- *(DTAM130-DTAM136: CAT II) The SA will ensure a scan is configured to perform a virus scan of the machine's local drive(s), using the following settings:*

BUFFER OVERFLOW PROTECTION		
TAB	***PARAMETER***	***REQUIRED SETTING***
Enable Buffer Overflow Protection	*Enable Buffer Overflow Protection* *Protection Mode* *Show the message dialog box when a buffer overflow is detected.*	*Enable* *Enable* *Enable*
Reports	*Log to File* *Limit to Size*	*Enable* *Enable* *100* [or higher]

Table B-7. Buffer Overflow Protection

B.2.7 Unwanted Programs Policy (Version 8.x only)

This table defines the types of unwanted programs to scan for but the actual scan settings much be enabled.

- *(DTAM150-DTAM152: CAT II) The SA will ensure a scan is configured to perform a virus scan of the machines's local drive(s), using the following settings:*

UNWANTED PROGRAM POLICY		
TAB	***PARAMETER***	***REQUIRED SETTING***
Detection	*Spyware* *Adware*	*Enable* *Enable*

Table B-8. Unwanted Program Policy

B.2.8 Access Protection Properties (Version 8.x only)

This item allows port blocking and definition of file shares. Specific guidance is not provided within this section as requirements. These parameters should be configured with an overall view of the machine in mind. In some cases multiple levels of port blocking within a machine can have a negative effect. If a personal firewall is already installed on the machine, the settings that control access protection mechanisms should be coordinated with the SA responsible for the personal firewall to ensure that overall machine configuration will control access appropriately.

APPENDIX C. WEB BROWSER PRODUCT SPECIFIC GUIDANCE

Currently, only three products are covered in this Appendix. Priority is given to Microsoft's Internet Explorer because it is installed with every Windows Operating System and Netscape because of a DoD licensing agreement. Firefox has been added because of the growing installation base within DoD.

C.1 Netscape Navigator

Navigator is a web browser client from Netscape Communications Corporation. Navigator has a number of security-related options that must be set. This document section is broken down into subsections that align loosely with the product menu structure. This allows for somewhat easier manual configuration when necessary.

This section includes configuration requirements for Navigator 7.x.

When implementing on more than a few desktop machines, System Administrators should consider the use of tools to automate configuration tasks. Tools such as the Netscape Client Configuration Kit (CCK) or Netscape Mission Control can reduce the effort required to customize and distribute the Navigator browser client software.

C.1.1 Software Maintenance

Netscape is no longer a vendor-supported product. Limited support is available for the Netscape Browser product through the DoD license agreement. Details about the DoD license agreement can be found at http://netscape.intelligent.net/disa/app.

NOTE: All patching and product support requirements (DTBG001-DTBG004) as detailed in *Section 5.1, Software Maintenance*, apply to Netscape.

The vendor's web site is http://channels.netscape.com/ns/browsers/default.jsp.

C.1.2 Navigator 7.x

- *(DTBN060-DTBN084: CAT II) The SA will ensure the Navigator 7.x Preferences parameters are configured according to the settings in the following table:*

NETSCAPE 7.x PREFERENCES SETTINGS		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
Navigator	*When Navigator starts up, display*	*Blank page* *[or]* *Home page*
	Home page – Location	*[If any, a trusted site or name of a local file]*
Navigator *-Downloads*	*When starting a download [Recommended]*	*Open the download manager* *[or]* *Open a progress dialog*
Privacy & Security *- Cookies*	*Cookie Acceptance Policy*	*Enable cookies based upon privacy settings (See note following table)*
Custom Cookie Settings (for all site types)	*First party Cookie* *Third party Cookie*	*Accept* *Reject*
Privacy & Security *- Forms*	*Save form data from web pages when completing forms*	*Disabled*
Privacy & Security *- Passwords*	*Password manager* *- Remember passwords* *Encrypting versus Obscuring* *- Use encryption when storing sensitive data*	*Disable* *Enable*
Privacy & Security *- Master Passwords [see note following table]*	*Change Master Password*	*[A user-specified value that conforms to CJCSM 6510.01, as possible.]*
	Master Password Timeout	*Every time it is needed*

NETSCAPE 7.x PREFERENCES SETTINGS		
CATEGORY	***PARAMETER***	***REQUIRED SETTING***
Privacy & Security *- SSL*	*SSL Protocol Versions* *- Enable SSL version 2* *- Enable SSL version 3* *- Enable TLS*	 *Enable [Preferred]* *Enable* *Enable* *[See cipher settings below]*
	SSL Warnings *- Loading a page that supports encryption* *- Loading a page that uses low-grade encryption* *- Leaving a page that supports encryption* *- Sending form data from an unencrypted page to an unencrypted page* *- Viewing a page with an encrypted/unencrypted mix*	 *Enable* *Enable* *Enable* *Enable* *Enable*
Privacy & Security *- Certificates*	*-Client Certificate Selection* *-Manage Security Devices*	*Ask Every Time* *Netscape Internal PKCS #11 Module* *[or]* *Netscape Internal FIPS PKCS #11 Module*
Validation	*OCSP (Online Certificate Status Protocol)*	*Use OSCP to validate only certificate that specify an OCSP service* *[or]* *Use OCSP to validate all certificate using this URL and signer – defined with valid service*
Advanced	*Enable features that help interpret web pages* *- Enable Java* *-XSLT*	 *Enable* *Disabled*
Advanced *- Software Installation*	*Manage Software Installations and Updates* *- Enable software installation*	 *Disable*

Table C-1. Netscape 7.X Preferences Settings

NOTE: The Navigator version 7.x Master Passwords options are used to provide protection of the use of user PKI certificates. The master password that secures the PKI certificates is also used by Navigator to protect information that is captured by the Form Manager and Password Manager components. Unlike client certificates that could be re-installed from source files, form and web password data is lost if the master password is reset. Sites should notify their users of this consideration.

These settings can be configured in Navigator from the Edit | Preferences dialog.

NOTE: To set the cookie security policy, click on the view button located next to the "Enable cookies based upon privacy setting" option, then select "Custom" as the predefined policy level.

It should be noted for CAs that do not support the Online Status Certificate Status Protocol, those CRLs should be imported into Netscape. Browsing to the CRL and clicking on the CRL to be installed accomplishes this. Select to automatically update the CRL and update every one day(s) before the Next Update date.

It is possible to enable specific cryptographic algorithms to be used during SSL browser sessions. Because these settings allow a user to specify a configuration in which an SSL session without encryption could be established, it is critical to ensure that proper settings are maintained.

The recommended settings for SSL v2 are listed in the following table.

NAVIGATOR 7.2.x SSL2 CIPHER SETTINGS	
CIPHER TYPE	***STATUS***
RC4 encryption with a 128-bit key	*Enable [Preferred]*
RC2 encryption with a 128-bit key	*Enable [Preferred]*
Triple DES encryption with a 168-bit key	*Enable [Preferred]*
DES encryption with a 56-bit key	*Enable [Preferred]*
RC4 encryption with a 40-bit key	*Disable [Preferred]*
RC2 encryption with a 40-bit key	*Disable [Preferred]*

Table C-2. NAVIGATOR 7x SSL2 Cipher Settings

- *(DTBN090-DTBN095: CAT II) The SA will ensure the settings for enabled ciphers for SSL3/TLS are configured as follows:*

NAVIGATOR 7.x SSL3/TLS CIPHER SETTINGS	
CIPHER TYPE	***STATUS***
RC4 encryption with a 128-bit key and an MD5 MAC	*Enable [Preferred]*
FIPS 140-1 compliant triple DES encryption and SHA-1 MAC	*Enable*

NAVIGATOR 7.x SSL3/TLS CIPHER SETTINGS	
CIPHER TYPE	***STATUS***
Triple DES encryption with a 168-bit key and a SHA-1 MAC	*Enable*
FIPS 140-1 compliant DES encryption and SHA-1 MAC	*Enable*
DES encryption with a 56-bit key and a SHA-1 MAC	*Enable*
RC4 encryption with a 56-bit key and a SHA-1 MAC	*Enable [Preferred]*
DES encryption in CBC mode with a 56-bit key and a SHA-1 MAC	*Enable [Preferred]*
RC4 encryption with a 40-bit key and an MD5 MAC	*Disable [Preferred]*
RC2 encryption with a 40-bit key and an MD5 MAC	*Disable [Preferred]*
No encryption with an MD5 MAC	*Disable*

Table C-3. NAVIGATOR 7.x SSL3/TLS Cipher Settings

The settings indicated as "*[Preferred]*" may be enabled or disabled at the site's discretion. While disabling these optional ciphers can result in failures to establish SSL sessions with some servers, it does increase the security of completed connections using stronger algorithms. The preferred options shown here are intended to allow interoperability with most servers while disallowing less secure (40-bit) connections. Disabling all of the optional settings, along with the use of the associated Netscape Internal FIPS PKCS #11 Module, is intended to permit a FIPS 140-1 compliant configuration.

These settings can be configured in Navigator from the Edit | Preferences | Privacy & Security | SSL | Edit Ciphers… dialog.

C.1.3 Netscape Plug-ins and Helper Applications

Navigator supports "Netscape Plug-ins" and "Helper Applications" as methods of extending the capabilities of the browser to handle file types beyond HTML. Vulnerabilities can be introduced when those components support the execution of mobile code. Specifically, actions are necessary when the plug-ins or applications do not have internal controls that restrict mobile code.

Netscape Plug-ins that support the execution of ActiveX controls have not provided the capability to disable unsigned ActiveX controls while enabling a user to permit appropriately signed controls to execute. Because of this deficiency, use of the Netscape ActiveX Plugin (aka Mozilla ActiveX Plugin) is prohibited by the DoD Mobile Code Policy; it must be uninstalled.

NOTE: This plugin is automatically included with the Netscape 7.x installations.

- *(DTBN100: CAT II) The SA will ensure Netscape Plug-ins support ActiveX controls are not installed.*

The installed Netscape Plug-ins can be reviewed in Navigator from the Help | About Plug-ins dialog or by entering "about:plugins" in Navigator's location field.

Helper Applications are defined within Navigator to link file types to other applications on the machine. Because many file types may contain some form of code, vulnerabilities can be introduced when the files are opened through the browser.

- For prohibited file types, it is necessary to take steps to ensure that a default Helper Application that executes the embedded code is not invoked. Navigator version 7.x uses the MIME Content Type in the file extension definitions in the Windows Registry to determine the Helper Application. If there is no MIME Content Type information, Navigator attempts to determine the proper MIME type from the file contents and either opens the file as text within the browser or prompts the user for a Helper Application to use. File types that are handled internally by the browser do not invoke a Helper Application.

- *(DTBN101: CAT II) The SA will ensure if any of the following file types are defined to Windows, the Content Type setting is blank or is associated with an application that does not execute the code in the file:*

NETSCAPE HELPER APPLICATION UPDATES	
FILE TYPE	***EXTENSION***
HTML Applications	*HTA*
Jscript Script File	*JSE*
JavaScript Program	*JS, MOCHA*
Scrap Object	*SHS*
VBScript Script File	*VBE, VBS*
Windows Script Component	*SCT, WSC*
Windows Script File	*WSF*
Windows Script Host Settings File	*WSH*

Table C-4. Netscape Helper Application Updates

The recommended Content Type values that meet this requirement are blank (i.e., no value specified), “text/plain”, or “application/x-javascript”. The use of “application/x-javascript” is permitted because the code is not executed in an external application, but within Navigator, and is subject to Navigator’s controls on code execution.

Windows Explorer can be used to manually display and configure the Content Type property. In Windows NT use the File Types tab of the View | Folder Options dialog in Windows Explorer. In Windows 2000 and XP use the File Types tab of the Tools | Folder Options dialog in Windows Explorer.

For some file types, providing the user an opportunity to cancel the open of the file provides adequate protection for most environments. Files that are opened with helper applications that include internal controls on code execution are good candidates for this technique.

Within Navigator's Helper Application support, it is possible to enable an open confirmation dialog. The property, enabled through the "Ask me before opening downloaded files of this type**"** setting, provides a notice to the user that allows them to open the file, save the file to disk, or cancel the file open task.

- *(DTBN102: CAT II) The SA will ensure if any of the following file types are defined in Navigator with Helper Applications, the "Ask me before opening downloaded files of this type" setting is enabled:*

NETSCAPE HELPER OPEN CONFIRMATION UPDATES	
FILE TYPE	***EXTENSION***
Adobe Acrobat Document, Forms Document	*PDF, FDF, XFDF*
LotusScript Library, Object, Source	*LSL, LSO, LSS*
Microsoft Excel Web Query File, Object Linking and Embedding file (OLE) DB Query File, Backup File, Worksheet, Template	*IQY, RQY, XLK, XLS, XLT*
Microsoft PowerPoint Template, Slide Show, Presentation	*POT, PPS, PPT*
Microsoft Word Document, Template, Backup Document	*DOC, DOT, WBK*
MS-DOS Batch File	*BAT*
PostScript	*PS, EPS*
WordPerfect (PerfectScript) Coach, Macro	*WCH, WCM, WB1, WB3*
Rich Text Format	*RTF*
WordPerfect (PerfectScript) Coach, Macro	*WCH, WCM*
Microsoft Access	AD, ADP, MDB, MDE
VISIO	VSS, VST, VSD, VSW
Shockwave	*DCR, DXR, DIR, SPL, SWF*

Table C-5. Netscape Helper Open Confirmation Updates

For Navigator version 7.x, the Edit | Preferences | Navigator | Helper Applications dialog shows entries based on the MIME type, but does not show entries for file types defined to Windows. Changes to the "Ask me before opening**…**" setting are stored in a user-unique preferences file named "prefs.js". If that file contains entries such as "browser**.**helperApps**.**neverAsk**.**openFile" for applications related to the file types above, the "Ask me before opening**…**" setting is not specified according to the requirement.

C.1.4 Certificates

As discussed earlier, digital certificates are used in the SSL protocol that supports secure browser sessions. Because the certificates are critical parts of the identification and authentication process, attention to the installed certificates is important.

- *(DTBG007: CAT II) The SA will ensure Browsers used to connect to Government servers are capable of 128-bit encryption and the use of SSL.*

It is strongly recommended that sites install Navigator, install and configure (by enabling the Advanced | Enable Java Plugin setting) the Sun Java Plug-in software, as a recommended solution to support the execution of mobile code that is signed with a DoD code-signing certificate. Additional details concerning the use of code signing certificates in Netscape is described in the *Developer's Guide for Using Mobile Code Technologies in Department of Defense and Intelligence Community Information Systems* document referenced in *Appendix A, Related Publications*.

For Navigator version 7.x, these characteristics can be verified in Navigator from the Help | About Netscape dialog. The capability for 128-bit encryption is indicated by the phrase, "*This version supports high-grade (128-bit) security…*"

- *(DTBG010: CAT II) The SA will ensure the certificate for the DoD Class 3 Root Certificate Authority and appropriate sublevel DoD CA Certs are installed.*

The DoD Class 3 Root CA certificate can be downloaded from the DoD PKI sites at http://dodpki.c3pki.chamb.disa.mil/ or http://dodpki.c3pki.den.disa.mil/.

The certificates for the DoD PKI External Certificate Authorities (ECAs) and Interim ECAs (IECAs) should be installed at the site's option.

User certificates should be installed in accordance with the instructions provided by the Local Registration Authority (LRA) or Trusted Agent (TA) that supplies them. In all cases, certificate use must be under password control. The settings required by the previous sections concerning Netscape Preferences, will ensure that this protection is active.

For Navigator version 7.x, the installed certificates can be verified in Navigator from the Edit | Preferences | Privacy & Security | Certificates | Manage Certificates dialog.

C.2 Microsoft Internet Explorer

Internet Explorer, known hereafter as IE, is a web browser client from the Microsoft Corporation. It is (currently) bundled in, and shares components with, each Microsoft operating system. IE also owns components used by other products such as Microsoft Outlook that render HTML documents for display. As a result, other products are impacted by the configuration parameters used by IE.

Because of these product relationships, the requirements in this section for configuration settings and product maintenance must be followed even when IE is not explicitly used as a browser on the machine.

When implementing on more than a few desktop machines, system administrators should consider the use of tools to automate configuration tasks. Tools such as the Internet Explorer Administration Kit (IEAK) can reduce the effort required to customize and distribute IE browser client software.

C.2.1 Software Maintenance

Microsoft's maintenance philosophy for IE currently includes service packs and patches. Service packs are planned collections of integrated maintenance that may address a diverse set of problems. Service Packs usually include maintenance that addresses security issues. Patches are provided as needed to correct individual problems.

In some cases the installation of updates to IE may include an update to the Windows Scripting Host (WSH) component. As indicated in *Section 3.5.1, File Type Handling Properties - Preventing Code Execution*, there are requirements relating to the Windows file type definitions that are associated with WSH. After the installation of updates to IE, the SA must ensure that the system still adheres to the requirements in *Section 3.5.1*.

NOTE: All patching and product support requirements (DTBG001-DTBG004) as detailed in *Section 5.1, Software Maintenance*, apply to Internet Explorer.

C.2.2 Internet Options

- *(DTBI001-DTBI020: CAT II) The SA will ensure the Internet Options parameters are configured according to the following settings:*

Table C-6. IE Internet Options

CATEGORY	***PARAMETER***	***REQUIRED SETTING***
General	*Home page – Address*	*about:blank [or] [A trusted site or the name of a local file]*

CATEGORY	*PARAMETER*	*REQUIRED SETTING*
Security	*Security level for this zone* *[applies to all zones]*	*Custom level* *[See Security Zone Settings in the following section.]*
	Local intranet – Sites *- Include all local (intranet) sites not listed in other zones* *- Include all sites that bypass the proxy server* *- Include all network paths (UNCs)*	*Disable* *Disable* *Disable*
Privacy	*First Party Cookies* *Third Party Cookies* *Always allow session cookies*	*Accept* *Block* *Checked*
Advanced	*When searching*	*Do not search from the Address bar* *[or]* *Just display the results in the main window*
	Check for signatures on downloaded programs	*Enable*
	Do not save encrypted pages to disk	*Enable* *[see note following table]*
	Use SSL 2.0	*Enable [Preferred]*
	Use SSL 3.0	*Enable*
	Use TLS 1.0	*Enable*
	Warn about invalid site certificates	*Enable*
	Warn if changing between secure and not secure mode	*Enable*
	Warn if forms submittal is being redirected	*Enable*

NOTE: As indicated above, the required setting for the "Do not save encrypted pages to disk**"** option is "enabled." In this configuration, web pages that are sent over encrypted

connections, that is connections using the SSL protocol, are not cached in IE's Temporary Internet files folder. The reason to prevent caching this data is the possibility that all or portions of the data are sensitive and the issue that access to the Temporary Internet files folder might not be appropriately restricted.

If it is determined that a user of a web application requires IE's caching capability and therefore cannot enable the "Do not save encrypted pages to disk" option, a mitigating action can be taken. This action requires the use of Windows' directory permissions to restrict access to the Temporary Internet files folder.

The Internet Options settings can be verified and set in IE from the General, Security, Privacy (IE 6.0), and Advanced tabs of the Tools | Internet Options dialog.

NOTE: Some of these tabs may not be displayed if the default Windows Registry settings have been changed.

The Advanced group of Internet Options controls some significant security parameters. To preserve the level of security, it is necessary to prevent arbitrary changes to the settings of these parameters.

- *(DTBI021: CAT III) The SA will ensure users are not permitted to make changes to the Advanced group of IE Internet Options.*

One method to prevent users from making changes is to set the value Advanced to 1 within the Windows Registry key [HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel].

C.2.3 Security Zones

The IE Security Zones feature puts web sites into groups for the purpose of applying security policy. When a user accesses a web site, the applicable Zone for that site is determined from IE parameters. In turn, each Zone can have unique security parameter settings. In general, the settings provide controls for the functions that are supported in web content. This content may consist of ActiveX controls and plug-ins, Java applets, scripts, cookies, and various other items. Because this content includes potentially malicious mobile code, the parameter settings are significant to security. Microsoft provides certain settings for each of the Zones according to a general level of risk.

By default, IE provides five Security Zones:

- Internet – The Internet zone is intended to include sites that are not in one of the other zones. The potential risk from these sites may be high.

- Local Intranet – The Local Intranet zone is intended to include sites that are local to the browser user. Settings can automatically place some sites in this zone. The potential risk from these sites is expected to be low.

- Trusted Sites – The Trusted Sites zone is intended to include those sites that have been specifically identified as secure, without regard to location. The potential risk from these sites is expected to be low.

- Restricted Sites – The Restricted Sites zone is intended to include those sites that have been specifically identified as not being secure, without regard to location. The potential risk from these sites is expected to be high.

- My Computer – The My Computer zone includes all client computer resources, usually the hard disk and removable media contents. The potential risk from this content is expected to be low.

Parameters for the Local Intranet zone allow sites to be placed there automatically on the basis of their domain name, their exclusion from proxy server requirements, or when their name expressed in Windows Uniform Naming Convention (UNC) syntax. This can degrade security by involuntarily assigning sites to a zone defined with less strict security settings.

As implemented by the requirements in *Section C.2.2, Internet Options*, options that allow sites to be automatically assigned to the Local Intranet zone are disabled.

The IAO should determine which sites are trusted and can be assigned to the Local Intranet zone or the Trusted Sites zone.

- *(DTBI022-DTBI136: CAT II) The SA will ensure the IE Security Zones are configured as securely as, or more securely than, the settings in the following table:*

Table C-7. Security Zone Settings

PARAMETER	***INTERNET ZONE***	***LOCAL INTRANET ZONE***	***TRUSTED SITES ZONE***	***RESTRICTED SITES ZONE***
Download signed ActiveX controls	*Disable*	*Prompt*		*Disable*
Download unsigned ActiveX controls	*Disable*	*Disable*		*Disable*
Initialize and script ActiveX controls not marked as safe	*Disable*	*Disable*		*Disable*
Run ActiveX controls and plug-ins	*Enable*	*Enable*		*Disable*
Script ActiveX controls marked safe for scripting	*Prompt*	*Prompt*		*Disable*
File download	*Enable*	*Enable*		*Disable*
Font download	*Prompt*	*Enable*		*Disable*

PARAMETER	***INTERNET ZONE***	***LOCAL INTRANET ZONE***	***TRUSTED SITES ZONE***	***RESTRICTED SITES ZONE***
Java Permissions (See notes on the Java permissions in the following text)	*Disable Java or Custom*	*Custom*		*Disable Java*
Access data sources across domains	*Disable*	*Prompt*		*Disable*
Allow META REFRESH	*Enable*	*Enable*		*Disable*
Display mixed content	*Prompt*	*Enable*		*Disable*
Do not prompt for client certificate selection when no certificate or only one certificate exists	*Disable*	*Disable*		*Disable*
Drag and drop or copy and paste files	*Prompt*	*Enable*		*Disable*
Installation of desktop items	*Disable*	*Prompt*		*Disable*
Launching programs and files in an IFRAME	*Disable*	*Prompt*		*Disable*
Navigate sub-frames across different domains	*Prompt*	*Enable*		*Disable*
Software channel permissions	*High safety*	*High safety*		*High safety*
Submit non-encrypted form data	*Prompt*	*Enable*		*Disable*
Userdata persistence	*Disable*	*Enable*		*Disable*
Active scripting	*Enable*	*Enable*		*Disable*
Allow paste operations via script	*Disable*	*Prompt*		*Disable*
Scripting of Java applets	*Prompt*	*Enable*		*Disable*
User Authentication – Logon	*Prompt for user name and password*	*Automatic logon with current username and password*	*Prompt for user name and password*	*Anonymous logon*

NOTE: The implementation of these settings does impact functionality in the IE and MS Outlook clients. This could negatively affect applications such as web server-based

applications and Microsoft Exchange-based workflow processes that depend on these functions.

To preserve the level of security, it is necessary to prevent arbitrary changes to these settings.

- *(DTBI170: CAT III) The SA will ensure users are not permitted to make changes to parameter settings for individual Security Zones.*

- *(DTBI171: CAT III) The SA will ensure users are not permitted to make changes to the sites that are assigned to specific Security Zones.*

These settings and restrictions can be verified and set in IE from the Security tab of the Tools | Options dialog unless display of the Security tab has been disabled in the Windows Registry.

One method to prevent users from making changes is to set the values Security_options_edit and Security_zones_map_edit to 1 within the Windows Registry key [HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings]. However, this change makes it impossible for the user even to view the security settings of each zone.

- *(DTBI150: CAT II) The SA will ensure the MS Java VM is not installed.*

NOTE: This is unsupported software. If this functionality is required, supported Java software will be used.

- *(DTBI200-DTBI201: CAT II) The SA will ensure that the MS Java VM permission settings are configured as securely as, or more securely than, the settings in the following table:*

JAVA VM PERMISSION SETTINGS				
CATEGORY	***PARAMETER***	***INTERNET ZONE***	***LOCAL INTRANET ZONE***	***TRUSTED SITES ZONE***
Unsigned Content	*Run Unsigned Content*	*Run in sandbox*		
	Additional Unsigned Permissions *- Access to all Files* *- Access to all Network Addresses* *- Execute* *- Dialogs* *- System Information* *- Printing* *- Protected Scratch Space* *- User Selected File Access*	*Disable* *Disable* *Disable* *Disable* *Disable* *Disable* *Disable* *Disable*		
Signed Content	*Run Signed Content*	*Prompt*		
	Additional Signed Permissions *- Access to all Files* *- Access to all Network Addresses* *- Execute* *- Dialogs* *- System Information* *- Printing* *- Protected Scratch Space* *- User Selected File Access*	*Prompt* *Prompt* *Prompt* *Prompt* *Prompt* *Prompt* *Prompt* *Prompt*		

NOTE: *If the Internet Zone Security Zone settings specify the **Java permissions** setting as **Disable Java**, it is not necessary to set the individual MS Java VM Permissions.*

These settings can be manually viewed or configured using the **Edit Permissions** tab that is accessed through the **Java Custom Settings** dialog in the **Custom Level** settings dialog for each individual Security Zone.

C.2.4 IE Cipher Settings

Cryptographic algorithms to be used during SSL browser sessions in IE are controlled through the Windows Registry. Because these settings could be configured to allow an SSL session without encryption, it is important to ensure that proper settings are maintained.

- *(DTBI151-DTBI153: CAT II) The SA will ensure the settings for enabled ciphers for SSL are configured as follows:*

IE SSL CIPHER SETTINGS	
CIPHER TYPE	***STATUS***
DES 56/56	*Enable*
NULL	*Disable*
RC2 128/128	*Enable [Preferred]*
RC2 40/128	*Disable [Preferred]*
RC2 56/128	*Disable [Preferred]*
RC4 128/128	*Enable [Preferred]*
RC4 40/128	*Disable [Preferred]*
RC4 56/128	*Disable [Preferred]*
RC4 64/128	*Enable [Preferred]*
Skipjack	*Enable [Preferred]*
Triple DES 168/168	*Enable*

Table C-8. IE SSL Cipher Settings

The settings indicated as "*[Preferred]*" may be enabled or disabled at the site's discretion. While disabling these optional ciphers can result in failures to establish SSL sessions with some servers, it does increase the security of completed connections using stronger algorithms. The preferred options shown here are intended to allow interoperability with most servers while disallowing less secure (40-bit) connections.

Only making changes to the appropriate Windows Registry keys can configure these settings. The keys are located under the following branch:

[HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

To enable a cipher for all protocols, set the DWORD value data of the Enabled value to 0xffffffff. To disable a cipher for all protocols, set the DWORD value data of the Enabled value to 0x0.

Please note that these registry keys may be used by software other than IE. On a Windows server machine this includes the Internet Information Services (IIS) web server.

- *(DTBI160: CAT II) The SA will ensure the settings for enabled hash algorithms for SSL are configured as follows:*

IE SSL HASH SETTINGS	
HASH TYPE	***STATUS***
MD5	*Enable [Preferred]*
SHA	*Enable*

Table C-9. IE SSL Hash Settings

Making changes to the appropriate Windows Registry keys is the only way these settings can be configured.

The keys are located under the following branch:

[HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes]

To enable a hash algorithm for all protocols, set the DWORD value data of the Enabled value to 0xffffffff. To disable an algorithm for all protocols, set the DWORD value data of the Enabled value to 0x0.

Please note that these registry keys may be used by software other than IE. On a Windows server machine this includes the Internet Information Services (IIS) web server.

C.2.5 ActiveX Download Management

When an ActiveX control is referenced in an HTML document, MS Windows checks to see if the control already resides on the client machine. If not, the control can be downloaded from a remote web site. This provides an automated delivery method for mobile code.

Assuming that downloading ActiveX controls is permitted by the Security Zone settings, there are two factors that influence the source location for ActiveX controls:

- The ActiveX control's OBJECT definition in the HTML document can include the "CODEBASE" keyword. "CODEBASE" can specify the web site and file location where the control can be downloaded.

- The "CodeBaseSearchPath" parameter in the Windows Registry specifies if the CODEBASE keyword should be honored and if additional web sites should be checked.

The "CodeBaseSearchPath" parameter can specify the keyword "CODEBASE" along with a series of web sites, separated by semi-colons. Each web site is enclosed in a greater than and less than sign. An example specification is:

"CodeBaseSearchPath"= "CODEBASE;<http://activex.microsoft.com/objects/ocget.dll>"

This example specifies that the location specified by the "CODEBASE" keyword on the HTML page be to be searched, followed by the site http://activex.microsoft.com/objects/ocget.dll to find the ActiveX control.

The default value provided with IE for the CodeBaseSearchPath parameter is:

CODEBASE;<http://activex.microsoft.com/objects/ocget.dll>;
<http://codecs.microsoft.com/isapi/ocget.dll>

The IAO should evaluate the impact of the value of the CodeBaseSearchPath parameter on their specific environment and require the SA to make modifications as needed. Possible modifications to the value of the parameter are as follows:

- Remove "CODEBASE" from the parameter string so that controls are not downloaded from sites specified in HTML documents.

- Add trusted web sites to the existing parameter string.

- Remove untrusted sites from the existing parameter string.

The recommended action for the "CodeBaseSearchPath" parameter is dependant on the risk evaluation for the site. For higher risk environments, the recommended action is to remove the "CODEBASE" entry and add trusted site(s) such as a patch server within the security enclave. For other environments the default value is usually appropriate.

The CodeBaseSearchPath parameter is defined in the Windows Registry, under the following branch:

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings]

C.2.6 Certificates

As discussed earlier, digital certificates are used in the SSL protocol that supports secure browser sessions. Because the certificates are critical parts of the identification and authentication process, attention to the installed certificates is important.

- *(DTBG007: CAT II) The SA will ensure Browsers used to connect to Government servers are capable of 128-bit encryption and the use of SSL.*

These characteristics can be verified in IE from the Help | About Internet Explorer dialog. The capability for 128-bit encryption is indicated by the phrase "*Cipher Strength: 128-bit.*"

- *(DTBG010: CAT II) The SA will ensure the certificate for the DoD Class 3 Root Certificate Authority and appropriate sublevel DoD CA Certs are installed.*

The DoD Class 3 Root CA certificate can be downloaded from the DoD PKI sites at http://dodpki.c3pki.chamb.disa.mil/ or http://dodpki.c3pki.den.disa.mil/.

The certificates for the DoD PKI External Certificate Authorities (ECAs) and Interim ECAs (IECAs) should be installed at the site's option.

User certificates should be installed in accordance with the instructions provided by the Local Registration Authority (LRA) or Trusted Agent (TA) that supply them. In all cases, certificate use must be under password control. For IE, two options should be selected when the certificate is imported. The first is "Enable strong private key protection." The second is setting the Security level to high for the Private Key Container.

The installed certificates can be verified in Internet Explorer from the Content tab of the Tools | Internet Options dialog.

C.2.7 Error Reporting Tool

The Internet Explorer Error Reporting tool is intended to provide diagnostic information to Microsoft when certain unrecoverable errors occur in IE. While the intent of this feature is to be helpful, the Department of Energy Computer Incident Advisory Capability group has identified potential information disclosure vulnerability. Information that is transmitted to Microsoft could contain a memory dump that includes parts of the document being viewed by the user. Since there is no apparent encryption scheme used in this feature, sensitive data could be intercepted in transit or disclosed inadvertently at the destination.

- *(DTBI140: CAT II) The SA will ensure the Internet Explorer Error Reporting tool is uninstalled or disabled.*

The Internet Explorer Error Reporting tool was an add-on to IE version 5.x, but was bundled with IE version 6.x. In addition, Windows XP provided a version of the tool that was integrated into the operating system. Because of these packaging differences, there are different ways to disable the tool.

- If the tool is installed with IE version 5.x, use the Control Panel | Add/Remove Programs dialog to uninstall it.

- If IE version 6.x is installed, a new Windows Registry value must be entered. Within the key **[**HKLM\Software\Microsoft\Internet Explorer\Main], create a DWORD value called IEWatsonEnabled and set it to 0.

- If IE version 6.x is installed on Windows XP, use the Control Panel | System | Advanced | Error Reporting dialog to select the Disable error reporting option.

C.3 FireFox

FireFox is an open source web browser client distributed by Mozilla Foundation. Please refer to Section 2.4 for information concerning Open Source and Freeware.

C.3.1 Software Maintenance

FireFox's maintenance is normally performed by releasing new versions of products. These updates are available for download from http://www.mozilla.org/.

NOTE: All patching and product support requirements (DTBG001-DTBG004) as detailed in *Section 5.1, Software Maintenance*, apply to FireFox.

C.3.2 Certificates/Encryption

FireFox provides functionality for encryption within a session. This is controlled through the dialog Tools|Options|Advanced|Security Tab dialog.

- *(DTBF010: CAT II) The SA will ensure FireFox is configured to allow use of SSL Version 2.0.*

- *(DTBF020: CAT II) The SA will ensure FireFox is configured to allow use of SSL Version 3.0.*

- *(DTBF030: CAT II) The SA will ensure FireFox is configured to allow use of TLS Version 1.0.*

FireFox also provides functionality for certificate management. This is also controlled through the dialog Tools|Options|Advanced|Security Tab dialog.

When a web site asks for a certificate for user authentication, FireFox must be configured to have the user choose which certificate to present. Also the DoD Root Certificate must be installed.

- *(DTBF050: CAT II) The SA will ensure FireFox is configured to ask which certificate to present to a web site when a certificate is required.*

- *(DTBG010: CAT II) The SA will ensure the certificate for the DoD Class 3 Root Certificate Authority and appropriate sublevel DoD CA Certs are installed.*

The DoD Class 3 Root CA certificate can be downloaded from the DoD PKI sites at http://dodpki.c3pki.chamb.disa.mil/ or http://dodpki.c3pki.den.disa.mil/.

FireFox includes the capability to use OSCP to validate certificates. The FireFox browser must be configured to use this protocol. This is controlled by setting either 'Use OSCP to validate only certificate that specify an OCSP service' or 'Use OCSP to validate all certificate using this URL and signer – defined with valid service'.

- *(DTBF060: CAT II) The SA will ensure FireFox is configured to use OSCP.*

C.3.3 File Handling within FireFox

FireFox provides the functionality to automatically download and execute a file. Because many file types may contain some form of code, vulnerabilities can be introduced when the files are opened through the browser. The dialog Tools|Options|Downloads|Download Actions Dialog lists the application that is associated with the file extension.

- *(DTBF100: CAT I) The SA will ensure if any of the following file types are listed in the Download actions dialog or they are associated with an application that does not execute the code in the file (such as Notepad):*

FILE TYPE	***EXTENSION***
HTML Applications	*HTA*
Jscript Script File	*JSE*
JavaScript Program	*JS, MOCHA*
Scrap Object	*SHS*
VBScript Script File	*VBE, VBS*
Windows Script Component	*SCT, WSC*
Windows Script File	*WSF*
Windows Script Host Settings File	*WSH*

Table C-10. FireFox Restricted Filetypes

- *(DTBF105: CAT I) The SA will ensure that the shell protocol is disabled.*

- *(DTBF110: CAT II) The SA will ensure if any of the following file types are listed in the Download actions dialog, the user is prompted before download.*

FIREFOX HELPER OPEN CONFIRMATION UPDATES	
FILE TYPE	***EXTENSION***
Adobe Acrobat Document, Forms Document	*PDF, FDF, XFDF*
LotusScript Library, Object, Source	*LSL, LSO, LSS*
Microsoft Excel Web Query File, Object Linking and Embedding file (OLE) DB Query File, Backup File, Worksheet, Template	*IQY, RQY, XLK, XLS, XLT*
Microsoft PowerPoint Template, Slide Show, Presentation	*POT, PPS, PPT*
Microsoft Word Document, Template, Backup Document	*DOC, DOT, WBK*
MS-DOS Batch File	*BAT*
PostScript	*PS, EPS*
WordPerfect (PerfectScript) Coach, Macro	*WCH, WCM, WB1, WB3*
Rich Text Format	*RTF*
WordPerfect (PerfectScript) Coach, Macro	*WCH, WCM*
Microsoft Access	AD, ADP, MDB, MDE

Table C-11. FireFox Open Confirmation

According to the DoD Mobile code policy, configuration settings must be put in place to disable automatic execution of certain types of mobile code.

FireFox relies on a plugin to properly execute ActiveX. This plug-in does not provide the capability to disable unsigned ActiveX controls while enabling a user to permit appropriately signed controls to execute. Because of this deficiency, use of this is prohibited by the DoD Mobile Code Policy.

- *(DTBF120: CAT II) The SA will ensure Plug-in for ActiveX controls is not installed.*

- *(DTBG016: CAT II) The SA will ensure the browser is configured to only allow Category 2 mobile code that is signed or received over a trusted channel.*

NOTE: If the Category 2 mobile code is not received over a secure channel, it must be executed within a constrained environment.

C.3.4 Miscellaneous Settings

This section describes settings that cover a range of FireFox browser security settings.

The browser home page parameter specifies the web page that is to be displayed when the browser is started explicitly and when product-specific buttons or key sequences for the home page are accessed. This is controlled from the Tools|Options Tab|General |Home Page dialog.

- *(DTBG017: CAT II) The SA will ensure the browser's home page is set to blank, a local file, or a trusted site.*

- *(DTBG009: CAT II) The SA will ensure options that provide warnings when a user switches from a secure (SSL-enabled) to a non-secure pages are enabled.*

In order to protect privacy and sensitive data, FireFox provides the ability to configure FireFox to not save data from forms. This is controlled from the Privacy – Saved Forms dialog.

- *(DTBF140: CAT II) The SA will ensure' the Saved information I enter in forms and the search bar' parameter is unchecked*

Firefox contains a master password that protects passwords that are saved. FireFox will be configured to not store passwords for sites. The master password will be set to protect any passwords or certificate information that is saved. These settings are controlled from the Tools|Options|Privacy tab.

Cookies are a way for web sites to track state within the application. FireFox controls cookies from the Options|Privay|Cookies dialog.

- *(DTBF150: CAT II) The SA will ensure FireFox is configured to not allow the user to save passwords.*

- *(DTBF160: CAT II) The SA will ensure FireFox is configured to have a master password.*

- *(DTBF170: CAT II) The SA will ensure FireFox is configured to warn when web sites try to install extensions or themes.*

Pop up windows need to be disabled. This is controlled from the Tools|Options|Content tab.

- *(DTBF180: CAT II) The SA will ensure FireFox is configured to block pop-up windows.*

JavaScript can make changes to the browser's appearance. This can help disguise an attack. This is controlled from the Options|Tools|Content|Java Script|Advanced dialog.

- *(DTBF181: CAT II) The SA will ensure FireFox is configured to disable JavaScript from moving or resizing windows.*
- *(DTBF182: CAT II) The SA will ensure FireFox is configured to disable JavaScript from raise or resize windows.*

- *(DTBF183: CAT II) The SA will ensure FireFox is configured to disable JavaScript from disabling or replacing context menus.*

- *(DTBF184: CAT II) The SA will ensure FireFox is configured to disable JavaScript from hiding the status bar.*

- *(DTBF185: CAT II) The SA will ensure FireFox is configured to disable JavaScript from changing the status bar text.*

Firefox allows the browser to access the Windows shell. This could allow access to the underlying system.

- *(DTBF190: CAT I) The SA will ensure FireFox is configured to disable the Windows shell protocol.*

This page is intentionally left blank.

APPENDIX D. E-MAIL CLIENTS PRODUCT SPECIFIC GUIDANCE

D.1 Microsoft Outlook

This section applies to the Microsoft e-mail clients - Outlook 2000, Outlook XP, and Outlook 2003. The term Outlook will be used in referring to all of these releases. Where relevant differences exist, the specific release is indicated. It should be noted that the Outlook clients share components with the Microsoft Internet Explorer web browser. Notations have been made where the shared components may be impacted by the e-mail client requirements.

The configuration guidelines for Outlook are divided into the following sections:

- Software Maintenance
- Security Zones
- Outlook Attachment Security
- Windows File Associations
- MS Office Macro Security.

D.1.1 Software Maintenance

Microsoft's maintenance philosophy for Outlook currently includes service releases, service packs, and patches. Because Outlook is a component of the MS Office suite, the service releases and service packs for MS Office provide Outlook maintenance. Service releases and service packs are planned collections of integrated maintenance that may address a diverse set of problems. Service Packs usually include maintenance that addresses security issues. Patches are provided as needed to correct individual problems.

Information about Microsoft Outlook patches can be found at http://www.microsoft.com/downloads/search.asp. These patches should be tested before general deployment to evaluate functional impact to the environment at a site.

NOTE: All patching and product support requirements (DTMG001-DTMG004) as detailed in *Section 6.1, Software Maintenance*, apply to Outlook.

D.1.2 Security Zones

Security Zones are a feature provided by Microsoft Internet Explorer (IE), but used by multiple applications. IE, Outlook, and Outlook Express all utilize settings maintained under Security Zones. Please refer to *Section C.2.3, Security Zones*, for details.

When Outlook processes a message in HTML format, the content is handled according to the controls in the Security Zone specified for Outlook. If not properly configured, malicious mobile code could be permitted to execute automatically.

- *(DTMO001: CAT II) The SA will ensure the Outlook client is configured to use the Restricted Sites Security Zone.*

The required configuration of the Restricted Sites Security Zone is specified in *Section C.2.3, Security Zones*.

These settings can be verified in Outlook from the Security tab of the Tools | Options dialog.

NOTE: The implementation of these settings does impact functionality available in the Outlook client. This could negatively affect applications such as Microsoft Exchange-based workflow processes that depend on these functions. In addition, web pages from sites designated by Internet Explorer settings to be in the Restricted Sites zone are also subject to the specified settings.

D.1.3 Outlook Attachment Security

The way Outlook attachment security is handled varies depending upon product version.

For Outlook 2000, this setting can be configured in Outlook from the Security tab of the Tools | Options dialog. The required value is High. This parameter provides a warning dialog and forces the user to save attachments to disk before they can be opened.

For Outlook XP, there is no configurable control on the client. Attachment security always operates as it does with the High setting in Outlook 2000.

For Outlook 2003, file types are defined to one of two security levels. The file types in Level 1 can't be changed. The file types in Level 2 can be changed at the Exchange Server level.

Attachments with a file type as defined in the Level 1 group will not be available to the user. Attachments with a file type as defined in the Level 2 group will force the user to save attachments to disk before they can be opened.

- *(DTMO002: CAT II) The SA will ensure Outlook is configured to set attachment security to the required parameters.*

It must be recognized that this feature does not remove the danger from malicious attachments. If a user saves the file to disk, the malicious code remains. Thus the feature is not a substitute for an anti-virus tool with current definitions.

D.1.4 Windows File Default Actions

When an e-mail attachment is opened in Outlook, settings configured under control of the Windows operating system dictate what occurs. Specifically, the default file type "Action" and the "Confirm open after download" setting specified in the Windows Registry are used to handle the file.

As required in *Section 3.5, File Type Handling Properties*, actions must be taken to ensure that files that may contain mobile code are properly handled. Details on updating the Windows file definitions are found in *Section 3.5, File Type Handling Properties*. Following the requirements in that section will allow Outlook to comply with the *Policy Guidance for use of Mobile Code*

Technologies in Department of Defense (DoD) Information Systems in order to reduce the risk of damage from malicious mobile code in e-mail attachments.

D.1.5 MS Office Macro Security

E-mail attachments often consist of one of the document types created by office automation products. Because the MS Office products hold a large market share, it is likely that any given e-mail attachment will be an MS Office document.

The embedded macro support in MS Office documents allows for a form of mobile code to be delivered through an e-mail attachment. This code comes in the form of a macro that is automatically invoked as the Office document is opened. As a result, it is important to control how the Office applications handle macros. Office macros are written in the Visual Basic for Applications (VBA) language. VBA is classified as a Category 2 mobile code technology as noted in *Section 5.3, Mobile Code*.

Section E.1.2, Macro Security, provides details on the facilities to control Office macro support and the required security settings. Following the requirements in that section will allow Outlook to comply with the *Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information Systems* in order to reduce the risk of damage from macro viruses.

D.1.6 HTML in E-mail

E-mail in HTML format can contain malicious mobile code. While there are other controls that address this issue, an Outlook feature introduced in Service Pack 1 (SP1) for Office XP can provide an additional defense. When enabled, the "Read as Plain Text" feature causes Outlook to render Rich Text Format (RTF) and HTML mail messages as plain text.

The feature is invoked for the message preview pane as well as open messages, but it does not apply to digitally signed or encrypted messages. Custom or third party solutions that rely on HTML or RTF messages can be negatively impacted.

To enable the "Read as Plain Text" feature create a DWORD value called "ReadAsPlain" and set it to 1 in the following Windows Registry branch:

[HKCU\Software\Microsoft\Office\10.0\Outlook\Options\Mail].

- *(DTMO003: CAT II) The SA will ensure Outlook E-mail clients are configured to read HTML context as text.*

Outlook 2003 also introduced a new feature that will allow SAs to block download and display of external content when displaying an HTML message. E-mail senders can imbed links to images or sounds within an e-mail message. When the e-mail message is opened, the mail sender can verify the users e-mail address. Using this function to block this activity can be helpful to avoid SPAM and protect user privacy.

These can be configured in Outlook 2003 from the Security tab of the Tools | Options dialog. This functionality is achieved by setting the Junk e-mail parameter to “Block external content in HTML.”

APPENDIX E. OFFICE AUTOMATION PRODUCT SPECIFIC GUIDANCE

E.1 MS Office

MS Office is the most commonly used office automation suite for desktop workstations. It has been offered in a number of configurations, differing in the specific applications that are bundled. A common implementation of Office includes the Word, Excel, PowerPoint, and Access applications. Issues that impact these applications are discussed in this section. The Outlook e-mail client is also a member of the Office family. Additional detailed information on Outlook is discussed in its own section, *Section D.1, Microsoft Outlook*. The Office 2000, Office XP, and Office 2003 versions of the suite are addressed in this document, but the applications' version numbers will only be referenced when a distinction is necessary.

One feature offered in Office is the use of file passwords. This feature applies to individual files, but is mentioned here because it does imply a level of security. Although the specific capabilities have varied among releases, there are currently options to require a password to open a document and to require a password to modify a document. Security that might be suggested by most of these options must be discounted. A number of free utilities exist that can be used to crack or otherwise obtain document passwords. Therefore, the Office file password features should not be considered adequate document security. Office XP and Office 2003 offers additional features including document encryption that may be more valuable in certain environments.

The Office applications provide multiple programmable interfaces. These include a macro language (Visual Basic for Applications), ActiveX control support, and documents in HTML with embedded scripts. In some instances, these different technologies can be combined in a single document. Actions that can be taken to address potential problems in these technologies are discussed in the following sections. For a more in-depth review of the capabilities and issues, refer to NSA's *Microsoft Office 2000 Executable Content Security Risks and Countermeasures*.

E.1.1 Software Maintenance

Microsoft's maintenance philosophy for Office currently includes service releases, service packs, and patches. Service releases and service packs are planned collections of integrated maintenance that may address a diverse set of problems. Service Packs usually include maintenance that addresses security issues. Patches are provided as needed to correct individual problems.

Information about Microsoft Office patches can be found at http://www.microsoft.com/downloads/search.asp. These patches should be tested before general deployment to evaluate functional impact to the environment at a site.

NOTE: All patching and product support requirements (DTOG001-DTOG004) as detailed in *Section 7.1, Software Maintenance,* apply to Office.

The configuration guidelines for Office are divided into the following sections:

- Macro Security
- ActiveX Controls
- HTML Format Documents
- Templates and Add-Ins
- Error Reporting Tool

E.1.2 Macro Security

Visual Basic for Applications (VBA) based macros can be embedded inside Office documents. It is possible to embed a macro that is automatically executed at the time the document is opened by the Office application or when other application *events*, such as document close, occur. When an attack is devised using this feature, the capability to embed a macro in any new documents that are created later is often used to further propagate the attack. VBA is classified as a Category 2 mobile code technology as noted in *Section 5.3, Mobile Code*. Following the requirements in this section allows Office to comply with the *Policy Guidance for Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems* in order to reduce the risk of damage from macro viruses.

Office 2000, Office XP, and Office 2003 offer macro virus protection known as the Security Level feature. This feature is used in conjunction with another capability—digitally signed macros. The Security Level feature supports three grades of security:

- High – Macros without digital signatures are automatically disabled. A warning dialog is displayed for digitally signed macros whose source has not been previously added to the "Trusted Sources' list. Once a source is trusted, as indicated by the user's acceptance at the warning dialog, all signed macros from that source are automatically enabled.

- Medium – A warning dialog is displayed, allowing the user to enable or disable macros. Digitally signed macros are handled as indicated under the High level.

- Low – All macro security warnings are turned off; all macros are enabled.

In addition, Office 2003 has added another level of macro security, Very High.

- Very High - VBA macros can run only if the Trust all installed add-ins and templates option is checked and the macros (signed or unsigned) are stored in a specific trusted folder on the user's hard disk. If all these conditions are not met, VBA macros cannot run under Very High security.

It should be noted that in many cases disabling macros does not prevent a user from reading or printing a document. As a result, the operational impact of using a more restrictive Security Level is not significant in every environment.

Office XP introduced a feature known as smart tags. Office 2003 also contains the smart tag feature. Smart tags are implemented in executable modules. They recognize data in documents and offer relevant actions to perform. Smart tag modules are packaged as Dynamic Link Library (DLL) elements that are installed within Windows. The use of smart tags is subject to the Office macro security level controls so that the selection of Very High (2003 only), High, Medium, or Low for macros is also applied to smart tags. This control includes applying the digital signature and Trusted Sources list processing rules in the same fashion as they are applied to macros.

Although the program code associated with smart tags is not embedded in Office documents, there are two ways in which code could get dynamically downloaded to a user's workstation. When the "More Smart Tags" button is selected in Office XP applications such as MS Word that support it, a web browser session is dynamically opened to a Microsoft site from which new or updated smart tags can be downloaded. The second way in which code could be downloaded is through data embedded in a document file. When the SmartTagDownloadURL property is defined with a valid web site location, the "Check for new actions" menu item in an existing smart tag would allow new code to be downloaded.

It is possible to control these two download capabilities by modifying Windows Registry entries. The key [HKCU\Software\Microsoft\Office\Common\Smart Tag] can contain entries CheckForNewSmartTags and CheckForNewActions with values that specify web site addresses.

The CheckForNewSmartTags entry is used to override the default location of "http://office.microsoft.com/office/redirect/10/smarttags.asp?HelpLCID=1033" for English language installations.

The CheckForNewActions entry is used to override sites specified in the SmartTagDownloadURL property in documents. Additional information about these controls is available with the documentation that accompanies Microsoft's Smart Tag Enterprise Resource Kit.

The recommended action for the CheckForNewSmartTags and CheckForNewActions parameters is dependant on the risk evaluation for the site. For higher risk environments, the recommended action is to set the entries to a trusted site(s) such as a patch server within the security enclave. For other environments the default configurations are usually appropriate.

Office 2003 has somewhat changed the smart tag feature. Individual smart tag execution can be enabled, disabled or crashed. The crashed status will occur if an error condition has occurred and can only be enabled from a change to the registry. To enable and disable a smart tag (other than if it is in a crash status), use the Smart Tag tab of the Tools | Autocorrect Options dialog and choose enable or disable.

The smart tag technology has not been formally reviewed for classification in terms of DoD mobile code categories. Therefore it may be designated as an emerging mobile code technology. This means that the technology cannot be used where it would effectively be enabling mobile code.

To control the use of Office macros and smart tags, the application settings for Security Level must be explicitly configured.

- *(DTOO001: CAT II) The SA will ensure Microsoft Word, Excel, PowerPoint, Access, Outlook and VISIO applications have the 'Macro Security Level' option set to Medium, High, or Very High.*

NOTE: The Very High or High setting is recommended, but not required due to backward compatibility requirements and ongoing digital signature implementations.

In Office 2000 and 2003, the macro Security Level setting and Trusted Sources list can be configured in each of the applications from the Security Level tab and Trusted Sources tab of the Tools | Macro | Security dialog.

In Office XP, the macro Security Level setting and Trusted Sources list can be configured in each of the applications from the Security Level tab and Trusted Sources tab of the Tools | Options | Security | Macro Security dialog.

It must be recognized that setting these options does not remove the danger from malicious attachments. Some settings still allow the user to open a document with a malicious macro enabled. Thus the option is not a substitute for an anti-virus tool with current definitions.

E.1.3 ActiveX Controls

ActiveX is a Microsoft technology intended to promote software reuse. ActiveX controls (known previously as OLE controls) are binary software components that add specific functions to a hosting application. By providing a standardized, object-based interface, these components can be used by multiple applications that need to perform the same functions. These controls are typically C programs and have access to all local resources on the client machine. ActiveX is classified as a Category 1 mobile code technology as noted in *Section 5.3, Mobile Code*.

Microsoft has distributed a number of ActiveX controls with Windows, Office, and Internet Explorer. In addition, ActiveX controls can be constructed using Microsoft development tools and a number of third-party controls have been created. It is the misuse of existing controls or the construction of malicious controls that can cause problems.

Each of the Office applications supports the use of ActiveX controls. The applications can create documents with embedded references to the controls and embedded controls themselves. Although referenced controls must be available on the system when they are invoked, it is possible to have them downloaded without direct user knowledge. Through references in HTML documents that are rendered by Internet Explorer components, ActiveX controls may be automatically downloaded over network connections. Note that the settings manipulated under Internet Explorer are used even if that is not the default browser defined to Windows.

The following actions can reduce potential vulnerabilities introduced by ActiveX controls:

- Ensure that any software that includes ActiveX controls receives available maintenance. There are patches that correct known vulnerabilities in controls provided with Office and Internet Explorer. Refer to the respective maintenance and vulnerabilities sections in this document.

- Ensure that the parameters for downloading ActiveX controls have been properly configured in Internet Explorer and in Windows. Please note that the IE configuration setting requirements must be followed even when IE is not explicitly used as a browser on the workstation. Refer to *Section C.2.3, Security Zones,* and *Section C.2.5, ActiveX Download Management,* for details.

E.1.4 HTML Format Documents

Word, Excel, and PowerPoint provide various levels of support for documents formatted in HTML, with the Office 2000 and XP versions providing more support than the earlier counterparts. All the applications can open and save documents in HTML format, with some HTML elements not processed. Components of Internet Explorer may be used to render some HTML elements.

Because documents in HTML format can support scripts and the invocation of ActiveX controls that could be applications supporting macros, the concerns already identified for those elements apply. Therefore, the following steps must be taken:

- Ensure that the applicable parameters have been properly configured in Internet Explorer and in Windows. Please note that the IE configuration setting requirements must be followed even when IE is not explicitly used as a browser on the workstation. Refer to *Section C.2.3, Security Zones*, and *Section C.2.5, ActiveX Download Management,* for details on restricting the download of ActiveX controls.

- Follow the guidelines in *Section E.1.2, Macro Security*, to configure the required settings for macro processing in Office applications.

E.1.5 Templates and Add-Ins

The Office applications can be customized through the use of templates and add-ins. A template can be thought of as a model document used as a basis for a new document with specific characteristics such as default text, specific fonts, and other pre-configured options. Templates are usually accessed through an application's File | New dialog. Office Add-ins are supplemental programs intended to customize or add features to an application. Add-ins can add new commands to program menus, tool bars, or object context menus.

Templates and add-ins are delivered in files. Microsoft provides a number of them with the Office suite; some third-party applications (such as Adobe Acrobat) add more. Because malicious code may be delivered in this form, it can be important to recognize them. The following table shows the file name extensions of templates and add-ins for the Office applications:

OFFICE/VISIO TEMPLATE AND ADD-IN EXTENSIONS		
OFFICE APPLICATION	***TEMPLATE FILE EXTENSION***	***ADD-IN FILE EXTENSION***
Access	.mdn	.mda, .mdt
Excel	.xlt, .xlthtml	.xla, .xll
PowerPoint	.pot, .pothtml	.ppa
Word	.dot, .dothtml	.wll
VISIO	.vst	

Table E-1. OFFICE/VISIO Template and Add-In Extensions

Templates and add-ins can include, or consist entirely of, VBA code. As with Office macros, this provides great flexibility with associated risks. Although different Office applications handle templates and add-ins differently in terms of warning dialogs for users, the available countermeasures are similar to those used for macros. Therefore, the following steps must be taken for template and add-in security:

- Follow the guidelines in *Section E.1.2, Macro Security*, to configure the required settings for macro processing in Office.

The Office 2000, XP and 2003 versions of Word, Excel, and PowerPoint provide an additional option that can enhance security for templates and add-ins. By disabling the "Trust all installed add-ins and templates**"** option, security warnings are applied to all add-ins and templates according to the current security level selected as follows:

- Very High (2003 only) – Add-ins that are not in trusted locations will not run.

- High – Add-ins that are not in trusted locations will not run unless they are signed from trusted sources.
- Medium – The user will be prompted to enable or disable macros that are not in trusted locations

This setting can be configured, from Trusted Sources tab of the
Tools | Options | Security | Macro Security dialog.

- *(DTOO002: CAT II) The SA will ensure Microsoft Word, Excel and PowerPoint applications disable the "Trust all installed add-ins and templates" option.*

E.1.6 Error Reporting Tool

The Error Reporting tool (also called the crash-reporting tool) is intended to provide diagnostic information to Microsoft when certain unrecoverable errors occur in Office applications. While the intent of this feature is to be helpful, the Department of Energy Computer Incident Advisory Capability group has identified potential information disclosure vulnerability. Information that is transmitted to Microsoft could contain a memory dump that includes parts of the document being viewed by the user. Since there is no apparent encryption scheme used in this feature, sensitive data could be intercepted in transit or disclosed inadvertently at the destination.

The Error Reporting tool is installed by default with Office XP. To disable the Error Reporting tool, set the DWORD value data of the values DWNeverUpload, DWNoExternalURL, DWNoFileCollection, and DWNoSecondLevelCollection to 1 within the Windows Registry key [HKCU\Software\Policies\Microsoft\Office\10.0\Common].

- *(DTOO003: CAT II) The SA will ensure the Error Reporting tool for Office XP and 2003 is uninstalled or disabled.*

NOTE: Office 2003 also has the capability to set up an organizational server for Office error messages. If an organizational server has been established for error reports and the Office application has been configured to use that server, the client error-reporting tool may be enabled.

E.1.7 Customer Experience Improvement Program

Office 2003 has the capability to allow the vendor to collect information about how products are being used. This usage information is then used to enhance the Office products. It is possible that this information could contain aggregate information that could be deemed sensitive. This feature will be disabled.

- *(DTOO004: CAT II) The SA will ensure the Customer Experience Improvement Program feature is disabled.*

This page is intentionally left blank.

APPENDIX F. LIST OF ACRONYMS

AIS	Automated Information System
C&A	Certification and Accreditation
CA	Certification Authority
CBC	Cipher Block Chaining
CCB	Configuration Control Board
CCK	Client Customization Kit
CDO	Collaboration Data Objects
CD-R	Compact Disk-Recordable
CD-RW	Compact Disk-ReWritable
CJCS	Chairman of the Joint Chiefs of Staff
COTS	Commercial-Off-The-Shelf
CVE	Common Vulnerabilities and Exposures
DAA	Designated Approving Authority
DECC	Defense Enterprise Computing Center
DECC-D	Defense Enterprise Computing Center - Detachment
DISA	Defense Information Systems Agency
DISAI	Defense Information Systems Agency Instruction
DMS	Defense Message System
DoD	Department of Defense
DoDD	Department of Defense Directive
DoS	Denial-of-Service
DSN	Defense Switched Network
E-mail	Electronic Mail
EAL	Evaluated Assurance Level
ECA	External Certificate Authority
FSO	Field Security Operations
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol with SSL
IASE	Information Assurance Support Environment
IAVM	Information Assurance Vulnerability Management
ICSA	International Computer Security Association
IE	Internet Explorer
IEAK	Internet Explorer Administration Kit
IEC	International Electrotechnical Commission
IECA	Interim External Certificate Authority
IIS	Internet Information Services
IM	Instant Messaging
IMAP4	Internet Messaging Access Protocol 4
IP	Internet Protocol

ISO	International Organization for Standardization
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
LRA	Local Registration Authority
MAC	Message Authentication Code
MD5	Message Digest 5
MIME	Multipurpose Internet Mail Extensions
MSDE	Microsoft SQL Server Desktop Engine
NIAP	National Information Assurance Partnership
NIPRNet	Non-Classified but Sensitive Internet Protocol Router Network
NSA	National Security Agency
NSO	Network Security Officer
OLE	Object Linking and Embedding
PCT	Private Communication Technology
PDA	Personal Digital Assistant
PKE	Public Key Enabling
PKI	Public Key Infrastructure
POP3	Post Office Protocol 3
RC2	Rivest's Cipher 2
RC4	Rivest's Cipher 4
RNOSC	Regional Network Operations and Security Center
RTF	Rich Text Format
SA	System Administrator
SHA	Secure Hash Algorithm
SIPRNet	Secret Internet Protocol Router Network
SMAPI	Simple Messaging Application Programming Interface
SMTP	Simple Mail Transfer Protocol
SP	Service Pack
SR	Service Release
SRR	Security Readiness Review
SRRDB	Security Readiness Review Database
SSL	Secure Sockets Layer
SSO	Systems Support Office
STIG	Security Technical Implementation Guide
TA	Trusted Agent
TASO	Terminal Area Security Officer
TLS	Transport Layer Security
UNC	Universal Naming Convention
URL	Uniform Resource Locator
VBA	Visual Basic for Applications
VM	Virtual Machine

VMS	Vulnerability Management System
WFP	Windows File Protection
WSH	Windows Scripting Host

This page is intentionally left blank.